LAUREA
AMMATTIKORKEAKOULU
Yhdessä enemmän

Teollisuuden ohjaus- ja automaatioympäristön kyberturvallisuussuunnitelma

Huhta, Jarmo

2017 Laurea Kerava

Laurea-ammattikorkeakoulu
Kerava

Teollisuuden ohjaus- ja automaatioympäristön kyberturvallisuus-suunnitelma

Jarmo Huhta
Tietojenkäsittelyn koulutusohjelma
Opinnäytetyö
Marraskuu, 2017

Laurea-ammattikorkeakoulu **Tiivistelmä**
Kerava
Tietojenkäsittelyn koulutusohjelma

Huhta, Jarmo

Kyberturvallisuussuunnitelma

Vuosi 2017 Sivumäärä 44

Tämän opinnäytetyön tarkoitus on esitellä menetelmä kyberturvallisuuden kehittämiseksi teollisuuden ohjaus- ja automaatiojärjestelmiä käyttävässä yrityksessä. Opinnäytetyön tuloksena syntyy kyberturvallisuussuunnitelma (kehityssuunnitelma) osaksi yrityksen normaalia toiminnan suunnittelua ja johtamisjärjestelmää.

Opinnäytetyössä keskitytään teollisuuden ohjaus- ja automaatiojärjestelmien kyberturvallisuuden kehittämiseen. Yrityksen hallinnollisten IT- ja tietojärjestelmien (esim. asiakashallinta- ja laskutusjärjestelmä) kyberturvallisuusasioita ei käsitellä tässä opinnäytetyössä.

Teoriaosan sijaan, opinnäytetyössä on esitelty suunnitelmassa viitekehyksinä käytetyt kyberturvallisuusalan keskeisimmät standardit.

Esiteltävän suunnitelman perusteella voidaan osoittaa, että teollisuuden ohjaus- ja automaatiojärjestelmien kyberturvallisuuden kehittäminen on jatkuva prosessi ja se kestää koko järjestelmien elinkaaren ajan. Lisäksi kyberturvallisuuden kehittäminen tulee olla osa yrityksen normaalia suunnittelu-, liiketoimintatoiminta- ja johtamisprosesseja.

Asiasanat: Kyberturvallisuus, tietoturvallisuus, IT-turvallisuus, teollisuuden ohjaus- ja automaatiojärjestelmä

Laurea University of Applied Sciences
Kerava
Business Information Technology

Abstract

Huhta, Jarmo

Cyber security plan

Year 2017 Pages 44

The purpose of this thesis is to present a method for developing cyber security in a company which utilize Industrial Control Systems (ICS/SCADA). The outcome of the thesis is a Cyber Security Plan (development plan) which will be used as part of company business planning and management system.

The focus of the thesis is the development of cyber security in industrial control systems. Cyber security of administrative IT and information systems (e.g. customer management and billing system) are not part of the thesis.

Theoretical section is replaced by section which presents well known and main standards in the area of cyber security.

Based on the presented plan development of ICS/SCADA system's cyber security is a continuous process and is present during the whole system life cycle. Also development of the cyber security shall be part of company business planning, business operation and management processes.

Keywords: Cyber security, Information security, IT security, ICS/SCADA system

Sisällys

Johdanto

Kyberturvallisuus on viimeisten vuosien aikana noussut kiinnostavaksi aiheeksi Suomessa niin tietoturvallisuuteen liittyvien julkaisujen ja lehtien kuin päivittäisten ilmestyvien sanomalehtienkin palstoilla. Osaltaan tähän ovat vaikuttaneet uutisoidut tietoturvallisuuspoikkeamat sekä kotimaassa että ulkomailla (Weiss 2010, 107), mutta myös Suomen Kyberturvallisuusstrategiasta annettu valtioneuvoston periaatepäätös ja sen luontiin liittynyt valmistelutyö sekä strategiassa edellytetyn toimeenpano-ohjelman kehittämiskohteet (Turvallisuuskomitean sihteeristö 2013).

Toimeenpano-ohjelmassa esitetään yhteensä 74 toimenpidettä, joiden tarkoitus on kehittää viranomaisten toimintatapoja ja siten parantaa väestölle ja yrityksille tarjottavia palveluja. Toimenpiteistä kolme (kohdat 72,73 ja 74) liittyvät erityisesti teollisuuden ohjaus- ja automaatiojärjestelmien kybersuojauksen ja tuotannon jatkuvuuden hallinnan kehittämiseen ja parantamiseen (Turvallisuuskomitean sihteeristö 2013). Edellä mainitut kehitystoimenpiteet on määritelty kuuluvaksi Huoltovarmuuskeskuksen tarjoamiin palveluihin.

Kyberturvallisuuden kehittäminen tulisi olla osana yrityksen toiminnan jatkuvaa kehittämistä. Kyberturvallisuuteen liittyvät tavoitteet ja prioriteetit tulisivat olla mukana yrityksen vuosittaisessa toimintasuunnitelmassa ja sen edellyttämässä resursoinnissa sekä osana vuosiraportointia.

1 Opinnäytetyössä käytetyt keskeiset käsitteet ja lyhenteet

Seuraavassa on kuvattu keskeiset käsitteet ja lyhenteet.

Kyber-	Kyber-sanaa käytetään lähes poikkeuksetta yhdyssanan määriteosana, ei yksinään. Sanan merkityssisältö liittyy yleensä sähköisessä muodossa olevan informaation käsittelyyn: tietotekniikkaan, sähköiseen viestintään (tiedonsiirtoon), tietojärjestelmiin tai tietokonejärjestelmiin. Yleensä vasta koko yhdyssanalla (määriteosan ja perusosan yhdistelmällä) voidaan ajatella olevan oma merkityksensä. Sanan kyber katsotaan tulevan kreikan kielen sanasta ”kybereo” (’ohjata’, ’opastaa’, ’hallita’).
Kybertoimintaympäristö; kyberympäristö	Toimintaympäristö, joka muodostuu yhdestä tai useammasta sähköisessä muodossa olevan datan tai informaation käsittelyyn tarkoitetusta tietojärjestelmästä. Esimerkkejä kybertoimintaympäristöistä ovat tietojärjestelmiin perustuvat ydinvoimalan ohjausjärjestelmä, elintarvikkeiden kuljetus- ja logistiikkajärjestelmä, liikenteen ohjausjärjestelmät sekä pankki- ja maksujärjestelmät.

Kyberturvallisuus	Tila, jossa kybertoimintaympäristöstä yhteiskunnan elintärkeille toiminnoille tai muille kybertoimintaympäristöstä riippuvaisille toiminnoille koituvat uhkat ja riskit ovat hallinnassa. Kyberturvallisuus voidaan ymmärtää myös tilaksi, jossa kybertoimintaympäristöön voidaan luottaa ja jossa sen toiminta turvataan. Kyberturvallisuuteen kuuluvat toimenpiteet, joilla voidaan ennakoivasti hallita ja tarvittaessa sietää erilaisia kyberuhkia ja niiden vaikutuksia. Kybertoimintaympäristön toiminnan häiriytyminen aiheutuu usein toteutuneesta tietoturvauhkasta, joten kyberturvallisuuteen pyrittäessä tietoturva on keskeinen tekijä. Tietoturvan lisäksi kyberturvallisuuteen pyritään mm. toimenpiteillä, joiden tarkoituksena on turvata häiriytyneestä kybertoimintaympäristöstä riippuvaiset fyysisen maailman toiminnot.
Tietoturva; tietoturvallisuus	Järjestelyt, joilla pyritään varmistamaan tiedon saatavuus, eheys ja luottamuksellisuus. Saatavuus tarkoittaa, että tieto on hyödynnettävissä haluttuna aikana. Eheys tarkoittaa tiedon yhtäpitävyyttä alkuperäisen tiedon kanssa ja luottamuksellisuus sitä, ettei kukaan sivullinen saa tietoa. Tietoturvan järjestelyjä ovat esimerkiksi kulunvalvonta, tilojen lukitus, asiakirjojen turvallinen säilytys ja hävitys, tietojen salaus ja varmuuskopiointi sekä palomuurin, virustorjuntaohjelman ja varmenteiden käyttö. Tietoturvaan kuuluu muun muassa tietoaineistojen, laitteistojen, ohjelmistojen, tietoliikenteen ja toiminnan turvaaminen. Tietoturvalla ja tietoturvallisuudella voidaan tarkoittaa myös oloja, joissa tietoturvariskit ovat hallinnassa.
Tietotekninen turvallisuus; IT-turvallisuus; ICT-turvallisuus	Menettelyt, joiden tarkoitus on tietojen, tietojärjestelmien ja tietoverkkojen tekninen suojaaminen. Pääpaino on teknisissä ratkaisuissa, tietoturvatuotteissa ja teknisessä osaamisessa.

2 Työn tausta

Lisääntyneen viranomaistoiminnan ja osittain myös säännöllisen medianäkyvyyden johdosta, kyberturvallisuus on noussut teollisuuden ohjaus- ja automaatiojärjestelmiä käyttävien yritysten ylimmän johdon kokousten asialistoille. Erityisesti huoltovarmuuskriittisten teollisuusyritysten tietoturvallisuudesta vastaavat saavat jatkossa tehtäväkseen määritellä kyberturvallisuuden merkitystä yrityksessä sekä suunnitella siihen liittyviä toimeenpano- ja kehityssuunnitelmia tai -ohjelmia. Yhtenä esimerkkinä edellisestä voidaan mainita elokuussa 2016 voimaan tullut Verkko- ja tietoturvadirektiivi, jossa EU:n jäsenvaltioiden on annettava ja julkaistava direktiivin noudattamisen edellyttämät lait, asetukset ja hallinnolliset määräykset viimeistään toukokuussa 2018 (LVM 2016). Direktiivin yleisenä tavoitteena on kasvattaa suojan tasoa verkko- ja tietoturvaloukkauksia, -riskejä ja -uhkia vastaan yhteiskunnan toimivuuden kannalta keskeisten palveluntarjoajien sekä tiettyjen digitaalisten palveluiden tarjoajien osalta.

Vaikka Kyberturvallisuusstrategia selkeyttikin kyberturvallisuuteen liittyviä käsitemalleja ja määritelmiä suhteessa tietoturvallisuuteen ja IT-turvallisuuteen, ovat käsitteet ja määritelmät edelleen vakiintumattomia, myös tietoturva-alan toimijoiden piirissä. Lisäksi kyberturvallisuuteen liittyy paljon kaupallisia intressejä, koska sitä käytetään usein myyntiargumenttina "uusille" tietoturvapalveluille ja -tuotteille.

2.1 Tavoite

Opinnäytetyön tavoitteena on esittää menetelmä kyberturvallisuuden kehittämiseksi teollisuuden ohjaus- ja automaatiojärjestelmiä käyttävässä yrityksessä. Esiteltävä menetelmä pitää sisällään myös ns. elinkaariajattelun, jonka tarkoitus on varmistaa, että kyberturvallisuusasiat on huomioitu niin ohjaus- ja automaatiojärjestelmien hankinnassa, käyttöönotossa, operatiivisessa käytössä, kuin niiden käytöstä poistossakin. Kyberturvallisuusstrategiassa olevien käsitteiden lisäksi, opinnäytetyössä esitellään käsitemalli yrityksen kyberturvallisuusasioiden ymmärtämisen helpottamiseksi suhteessa tieto- ja IT-turvallisuuteen.

2.2 Tutkimuskysymykset

Opinnäytetyössä määritellyn tavoitteen ja rajauksen perusteella, opinnäytetyöhön on määritelty seuraavat tutkimuskysymykset.

1. Miten kyberturvallisuusasioiden kehittäminen tulisi liittää osaksi yrityksen johtamisjärjestelmää?

Kyberturvallisuus ja sen kehittäminen eivät ole olleet perinteisesti teollisuuden ohjaus- ja automaatiojärjestelmiä käyttävien toimijoiden prioriteettilistalla. Usein luottamus toimittajiin on ollut rajaton tietoturva-asioissa. Tyypillisesti asia saa (johdon) huomion, kun ohjaus- ja automaatiojärjestelmien parissa tapahtuu esim. tietoturvapoikkeama, josta taas aiheutuu suunnittelemattomia käyttökatkoksia ja siten taloudellisia seuraamuksia.

2. Miten kyberturvallisuusasiat tulisivat huomioiduksi koko ohjaus- ja automaatiojärjestelmien elinkaaren ajan?

Verrattuna yrityksen hallinnollisen liiketoimintasovelluksen (esim. asiakas- tai henkilöstöhallintajärjestelmä) elinkaareen, teollisuuden ohjaus-ja automaatiojärjestelmien käyttöikä on usein paljon pitempi. Kun liiketoimintasovellukset tulevat elinkaarensa loppuun 5-7 vuoden käytön jälkeen, voidaan ohjaus-ja automaatiojärjestelmiä käyttää jopa yli 20 vuotta. Pitkä elinkaari asettaakin erityisiä haasteita järjestelmin tietoturvan hallinnalle, koska järjestel-

mään liittyvä osaaminen, toimittajatuki ja ylläpito voivat olla rajallisia elinkaaren loppuvaiheilla.

3. Mitä kyberturvallisuudella tarkoitetaan ohjaus- ja automaatiojärjestelmiä käyttävässä yrityksessä?

Aiheen ympärillä liikkuu monenlaisia käsitteitä ja termejä, jotka ovat usein kaupallisista lähtökohdista johdettuja eli ns. myyntiargumentteja. Kyberturvallisuus ei ole itseisarvo yrityksessä. Se on yksi toiminto, jonka tarkoitus on varmistaa organisaation liiketoimintaedellytykset niin normaali kuin poikkeustilanteissakin. Tämä tarkoittaa mm. sitä, että kyberturvallisuuteen liittyvät päätökset täytyvät olla liiketaloudellisesti perusteltuja, kuten mikä tahansa muukin kehittämiskohde.

2.3 Aihealueen rajaus

Opinnäytetyössä käsiteltävä alue on rajattu teollisuuden ohjaus- ja automaatiojärjestelmiä käyttävän yrityksen kyberturvallisuuden kehittämiseen. Opinnäytetyössä ei käsitellä yrityksen hallinnollisia tieto- tai IT-järjestelmiä (esim. sähköpostijärjestelmä, asiakas- ja laskutusjärjestelmät) vaan ainoastaan teollisuuden ohjaus- ja automaatiojärjestelmiä (ICS/SCADA).

3 Tutkimusmenetelmät

Kyberturvallisuutta käsiteltäessä tutkimukselliset kysymykset, jotka alkavat sanoilla mitä, miksi, miten ja kuka/ketkä ovat merkityksellisempiä kuin ne kysymykset, jotka alkavat sanoilla kuinka paljon/monta/vähän. Tietysti tämä ei ole aivan mustavalkoinen asia. Esimerkiksi kyberturvallisuuden mittaamiseen/kyvykkyyteen liittyvät asiat saattavat olla toistettavissa ja vertailtavissa, kunhan valittu mittari on yksiselitteinen ja selkeä.

Kyberturvallisuus aiheena on vielä niin epäkypsä, joten aihetta tarpeeksi yleistäen voidaan joidenkin aiheeseen liittyvien asioiden ennustamista, selittämistä ja ymmärtämistä helpottaa ja parantaa. Opinnäytetyössä esiteltävän kyberturvallisuuden kehittämismallin/konseptin/teorian tarkoitus on kehittää aiheeseen liittyvää ymmärrystä.

Opinnäytetyön aloittaminen ei edellytä kattavaa kirjallisuuskatsausta. Katsaus suoritettiin opinnäytetyön kirjoittamisen edetessä. Keskeisin tietojenkeruun keino oli omat havainnot ja kokemukset.

Opinnäytetyö on subjektiivinen eli aiheeseen liittyvät taustat ja tarkoitukset, teoreettiset lähestymistavat, eri määrittelyt ja menetelmät sekä eettiset ja luotettavuuteen liittyvät ky-

symykset perustuvat kirjoittajan omiin tulkintoihin, käsityksiin ja kokemuksiin kyberturvallisuudesta. Kyberturvallisuudesta ymmärretään vielä melko vähän ja sen merkityksestä sekä vaikutuksista ei olla päästy vielä yhteisymmärrykseen, joten aiheen henkilökohtaisesta näkemyksestä tai asenteesta riippumaton, puolueeton, tasapuolinen ja yleispätevä (objektiivinen) käsittely ei ole välttämättä mielekästä. Kirjoittajalla on läheinen suhde kehitettävään asiaan (kyberturvallisuus) eli kirjoittaja on osa kehittämisprosessia. Opinnäytetyön luotettavuuden ja uskottavuuden varmistamiseksi, on aihetta pyritty käsittelemään ilman henkilökohtaisia uskomuksia, asenteita ja arvostuksia.

3.1 Kvantitatiivinen ja kvalitatiivinen tutkimus

Opinnäytetyössä esiteltävän suunnitelman tarkoitus on kehittää teollisuuden ohjaus- ja automaationympäristön kyberturvallisuuden varmistamiseen liittyviä käytäntöjä, joten kyseessä on kehittämistutkimus. Kehittämistutkimus on tutkimusmenetelmä, jolla ei ole varsinaisesti omaa metodologiaansa, vaan käytettävä lähestymistapa valitaan aina tilanteen mukaan. Opinnäytetyössä on käytetty kvalitatiivisesta (laadullista) tutkimusmenetelmää, sillä Kanasen mukaan se on paras vaihtoehto, kun tutkittavasta ilmiöstä ei ole teoriaa (Kananen 2014, 16). Kanasen mukaan laadullinen tutkimus ei pyri yleistämään kuten määrällinen tutkimus, joka taas edellyttää hyvää tietämystä tutkittavasta ilmiöstä ja teoriasta.

Opinnäytetyössä hyödynnetään kyberturvallisuuteen liittyviä standardeja sekä aiempia teorioita, tutkimuksia ja julkaisuja. Tämä on ominaista määrälliselle tutkimukselle. Lisäksi käytettävien käsitteiden määrittely ja opinnäytetyön osa-alue liittyen kyberturvallisuuden mittaamiseen ovat myös tyypillisiä määrällisessä tutkimusmenetelmässä. Laadullista tutkimusmenetelmää käytetään, kun kyberturvallisuuden merkitystä kuvataan tarkemmin ja syvällisemmin osana suurempaa (tieto)turvallisuuskontekstia.

Kyberturvallisuuden ympärillä ei ole olemassa yhtä tieteellistä/teoreettista viitekehystä, jota opinnäytetyössä voitaisiin testata ja/tai todentaa. Kirjoittaja näkeekin asian niin että, työ osaltaan on kehittämässä kyberturvallisuuden ympärille syntyvää teoriapohjaa. Tutkittaessa kyberturvallisuutta, ei ole olemassa absoluuttista totuutta eikä kriittisiä pisteitä. Käytettävissä oleva aineisto on sitä mitä se tutkimus/kirjoitus hetkellä on ja tulkinta kyberturvallisuudesta jakautuu koko tutkimusprosessin ajalle.

3.2 Tutkimuksen reliaabelius ja validius

Opinnäytetyön kehittämistutkimuksen luotettavuutta arvioitaessa nousivat esiin validiteetti- ja reliabiliteettikysymykset, joita Kanasen mukaan käytetään tieteellisen tutkimuksen mittareina (Kananen 2014, 147). Validiteetti voidaan jakaa ulkoiseen ja sisäiseen validiteettiin si-

ten, että ulkoisella validiteetilla tarkoitetaan tutkimuksen yleistettävyyttä; onko se yleistettävissä ja mihin ryhmiin. Sisäinen validiteetti puolestaan tarkoittaa tutkimuksen omaa luotettavuutta. Reliabiliteetti tarkoittaa validiteetin tapaan luotettavuutta, mutta sen sisältö viittaa tutkimuksen toistettavuuteen. Tutkimuksen reliaabelius voidaan varmistaa monella eri tavalla. Jos useampi arvioija toteaa samanlaisen tuloksen, niin tulos on silloin reliaabeli, tai tutkittavana oleva kohde tutkitaan eri aikoina ja päädytään samaan tulokseen, voidaan silloin todeta tulokset reliaabeleiksi.

Opinnäytetyössä ei tavoitella mitattavissa olevia tai tilastollisia analyyseja. Tulokset ovat enemmänkin ideoita, ajatuksia ja lukijoiden tulkittavissa ja sovellettavissa. Lisäksi tulokset liittyvät aihekokonaisuuksiin kuten prosessit, organisaatiot ja vastuut. Opinnäytetyön lopputulosten saavuttaminen ei edellytä jonkinlaisten työkalujen/mittareiden/instrumenttien käyttöä. Toisaalta tulosten saavuttaminen vaatii hyvää kommunikointia ja havaintojen tekemistä.

4 Opinnäytetyössä käytetyt tietoturvastandardit ja muut viitekehykset

Opinnäytetyössä on käytetty useita eri tietoturvaan joko suoraan tai välillisesti liittyviä kansainvälisiä tietoturvastandardeja. Niille kaikille on tunnusomaista toiminnan jatkuva kehittäminen, prosessikeskeisyys sekä kehittämisen johtamisen (Leadership) tärkeys. Näitä standardeja voidaan pitää myös teoreettisena viitekehyksenä tälle opinnäytetyölle.

4.1 PDCA-malli

PDCA (plan-do-check-act) -malli (sykli) on yksi keskeisiä työkaluja jatkuvassa parantamisessa, laatujohtamisessa ja prosessinkehittämisessä. Sitä kutsutaan myös Demingin tai Shewhartin ympyräksi/pyöräsi. PDCA:n kehitti Dr W. Edwards Deming, jota pidetään myös modernin laatuvalvonnan keksijänä. PDCA:n konsepti perustuu tieteelliseen metodiin, jonka kehitti Francis Bacon 1620–luvulla.

4.2 ITIL-dokumenttikokoelma

ITIL (Information Technology Infrastructure Library) on dokumenttikokoelma käytäntöjä IT-palveluiden hallintaan ja johtamiseen. ITIL on globaalisti tunnustettu prosessikehys, jonka kehitys alkoi Englannissa valtionhallinnon hankkeena 1980-luvulla. ITIL soveltuu kaikenkokoisten yritysten IT-prosessikehykseksi. Pääpaino on IT-palveluiden johtamisessa prosessien avulla. ITIL on kattava prosessikirjasto, ja sisältää parhaita käytäntöjä ja malleja IT-johtamisen prosesseille. ITIL:n nykyinen kokonaisuus julkistettiin kesäkuussa 2007 ja päivitettiin kesällä 2011.

4.3 COBIT-kontrolli- ja -viitekehys

COBIT (Control Objectives for Information and Related Technology) on kontrolli- ja viitekehys tietotekniikan hallinnan ja johtamiskäytäntöjen kehittämiselle, toteutukselle, seurannalle ja parantamiselle. COBIT-viitekehyksen julkaisusta vastaa IT Governance Institute ja Information Systems Audit and Control Association (ISACA). Viitekehyksen tavoitteena on tarjota yhteinen kieli yritysten johtajille kommunikoida keskenään tavoitteista ja tuloksista. Vuonna 1996 julkaistussa alkuperäisessä versiossa keskityttiin pääosin tilintarkastukseen. Vuonna 2013 julkaistussa uusimmassa versiossa painotetaan sitä, että tietohallinto voi olla osana varmistamassa yrityksen liiketoimintamenestystä.

4.4 ISO/IEC 27000-sarja

ISO/IEC 27000 on sarja ISO:n (International Organization for Standardization) ja IEC:n (International Electrotechnical Comission) julkaisemia standardeja, jotka määrittävät parhaita käytäntöjä koskevia suosituksia tieturvallisuuden ja tietoriskien hallinnasta sekä valvonnasta ja tietoturvallisuuden hallintajärjestelmästä. Standardisarja on samankaltainen laadunvalvonta- (ISO 9000) ja ympäristönsuojelujärjestelmän (ISO 14000) kanssa. Standardisarja kattaa kaiken tyyppiset organisaatiot (esim. kaupalliset yritykset, valtion virastot, voittoa tavoittelemattomat organisaatiot) erikokoiset yritykset (pienistä aina monikansallisiin yrityksiin) sekä kaikkiin toimialoihin tai markkinoihin (esim. vähittäismyynti, pankki, puolustus, terveydenhuolto, koulutus ja hallinto).

4.4.1 ISO/IEC 27001-standardi

ISO/IEC 27001 on standardi tietoturvallisuuden hallintajärjestelmästä. Se sisältää joukon tietoriskien hallintaan liittyviä toimintoja, joita standardissa kutsutaan tietoturvariskeiksi. Tietoturvallisuuden hallintajärjestelmä on kokonaisvaltainen johtamisen viitekehys, jonka avulla organisaatio tunnistaa, analysoi ja minimoi sen tietoturvariskit. Hallintajärjestelmällä varmistetaan, että turvallisuusjärjestelyt hienosäätyvät vastaamaan turvallisuusuhkien, haavoittuvuuksien ja liiketoiminnan vaikutusten muutoksiin.

4.4.2 ISO/IEC 27002-standardi

ISO/IEC 27002 on standardi, joka määrittää suositukset hyvistä tietoturvakäytännöistä sellaisille tahoille, jotka ovat vastuussa tietoturvallisuuden hallintajärjestelmän suunnittelusta, käyttöönotosta tai ylläpidosta. Standardi määrittää tietoturvakontrollit, joilla hallitaan tietojen luottamuksellisuuteen, eheyteen ja käytettävyyteen liittyviä riskejä. Organisaatiot, jotka

ovat ottaneet käyttöön ISO/IEC 27002:n, on arvioitava tietoihinsa liittyvät riskit, selkeytettävä niiden kontrollitavoitteet ja sovellettava asianmukaisia kontrollitoimenpiteitä.

4.4.3 ISO/IEC 27019-standardi

ISO/IEC 27019 on standardi, joka sisältää ISO/IEC 27002 –standardiin perustuvia tietoturvallisuuden hallintaan liittyviä hyviä käytäntöjä, joita sovelletaan energia-alalla käyttämiin teollisuuden ohjaus- ja automaatiojärjestelmiin. Standardin tavoite on ISO/IEC 27000 -standardisarjan laajentaminen prosessinohjausjärjestelmien ja automaatiotekniikan alalle, jolloin energia-alan toimijat voivat toteuttaa standardoidun tietoturvallisuuden hallintajärjestelmän ISO/IEC 27001 -standardin mukaisesti, aina liiketoiminnasta prosessinohjaustasolle. Standardin soveltamisala kattaa prosessinohjausjärjestelmät, joita energia-alan toimijat käyttävät sähkön, kaasun ja lämmön tuotannon, siirron, varastoinnin ja jakelun valvontaan ja seurantaan yhdessä tukiprosessien valvonnan kanssa.

4.5 ISA/IEC-62443-standardi

ISA/IEC-62443 (ent. ISA-99) on sarja ISA:n (International Society for Automation) ja IEC:n (International Electrotechnical Comission) standardeja ja teknisiä raportteja, jotka määrittävät menettelyt turvallisten teollisuuden ohjaus- ja automaatiojärjestelmien toteuttamiseksi. Tämä standardi koskee loppukäyttäjiä eli järjestelmien omistajia, järjestelmäintegraattoreita, turvallisuusasiantuntijoita ja järjestelmätoimittajia (vastaavat teollisuuden ohjaus- ja automaatiojärjestelmien valmistuksesta, suunnittelusta, toteuttamisesta tai hallinnasta).

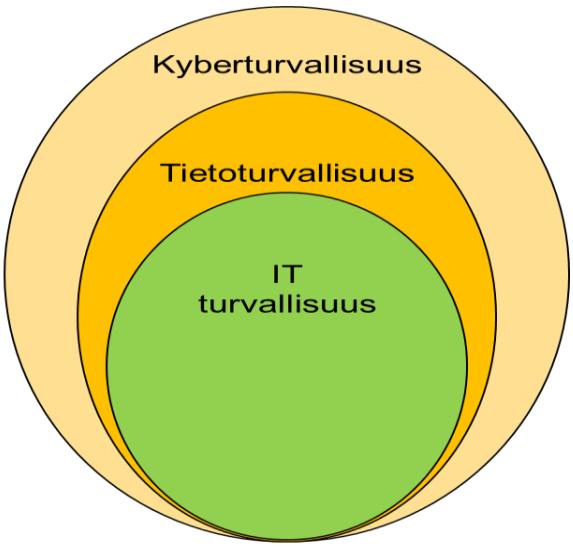
4.6 ISF SoGP-tietoturvaopas

ISF:n (Information Security Forum) julkaisema SoGP (Standard of Good Practice) on käytännöllinen ja kattava opas organisaatioiden ja toimitusketjujen tietoturvariskien tunnistamiseen ja hallintaan. Se vastaa ISO/IEC 27000 -standardien mukaista tietoturvallisuuden hallintajärjestelmää koskevia vaatimuksia. SoGP tarjoaa laajemman ja syvemmän kattavuuden ei pelkästään ISO/IEC 27002 -standardissa määrittämiin tietoturvakontrolleihin, vaan myös pilvitietojärjestelmiin, kuluttajalaitteisiin ja turvallisuusjohtamiseen. Opas kattaa myös kaikki COBIT:n aiheet ja on yhdenmukainen myös muiden asiaankuuluvien standardien ja lainsäädännön kanssa, kuten PCI DSS -standardi ja Sarbanes Oxley -laki.

5 Kyberturvallisuuden suhde tieto- ja IT-turvallisuuteen

Tässä luvussa on kuvattu kyberturvallisuuden suhdetta tieto-ja IT-turvallisuuteen. Mukaan on otettu myös muita organisaation turvallisuuteen liittyviä osa-alueita, kokonaiskuvan ja asian laaja-alaisuuden hahmottamiseksi. Mainittakoon vielä, että esitetty rakenne on kirjoittajan oma näkemys asiasta eikä se perustu välttämättä mihinkään vallitsevaan tai yleisesti hyväksyttyyn malliin.

Seuraavassa kuvassa käsiteltävät osa-alueet on kuvattu yhtenä rakenteena.



[1]

Kuva 1: Kyberturvallisuus suhteessa tieto- ja IT-turvallisuuteen

5.1 Kyberturvallisuus

Kyberturvallisuus keskittyy organisaation kriittisten toimintojen keskinäisriippuvuuteen, toimivuuteen ja verkottuneen toimintaympäristön tietoturvallisuuteen kokonaisuutena. Painotus on organisaation toiminnan jatkuvuuden varmistamisessa.

5.2 Tietoturvallisuus

Tietoturvallisuus huomioi organisaation tietojen suojaamisen laaja-alaisesti riippumatta tiedon olomuodosta, sijainnista tai käsittelytavasta. Painotus on organisaation tietojen luottamuksellisuudessa, eheydessä ja käytettävyydessä. Kokonaisvaltainen näkökulma, jossa otetaan huomioon organisaation tavoitteet, ihmiset, prosessit, teknologian ja ulkoiset riippuvuudet.

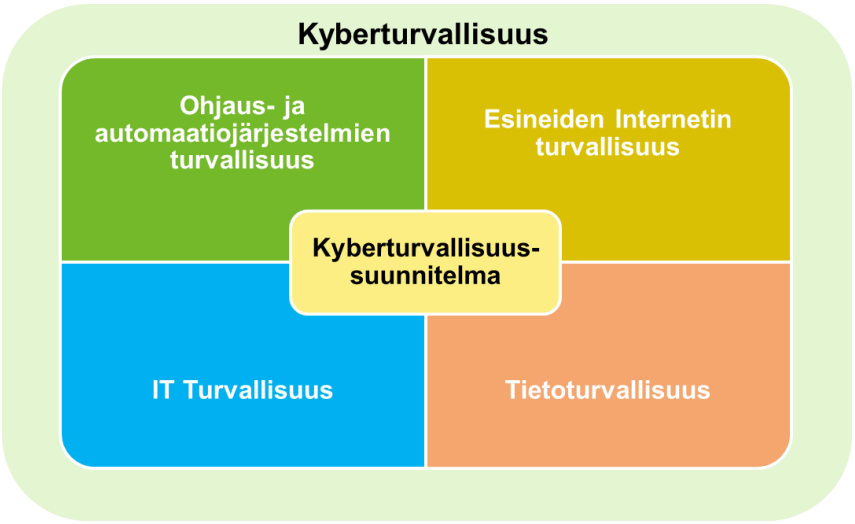
5.3 IT-turvallisuus

IT-turvallisuus (Tietotekninen turvallisuus, ICT-turvallisuus) keskittyy organisaation tietojen, tietojärjestelmien ja tietoverkkojen tekniseen suojaamiseen. Painotus on teknisissä ratkaisuissa, tietoturvatuotteissa ja teknisessä osaamisessa.

5.4 Vaihtoehtoinen jaottelu ja muut osa-alueet

Kuten opinnäytetyön taustoituksessa kuvattiin, ei kyberturvallisuudesta käsitteenä ja suhteessa muihin alan käsitteisiin ole kansainvälisesti sovittua yhteisymmärrystä tai mallia. Seuraavassa onkin kirjoittajan käyttämä rakenne kokonaisuuden hahmottamisen helpottamiseksi ja johtamisen apuvälineenä.

Seuraavassa kuvassa käsiteltävät osa-alueet on kuvattu kirjoittajan käyttämänä rakenteena.



Kuva 2: Kyberturvallisuussuunnitelma ja kyberturvallisuuden osa-alueet

5.4.1 Ohjaus-ja automaatiojärjestelmien turvallisuus

Ohjaus-ja automaatiojärjestelmien turvallisuus keskittyy organisaation ohjaus-ja automaatioympäristöissä käytettyjen tietojärjestelmien, järjestelmien ja verkkojen tekniseen suojaamiseen. Fokus ohjausjärjestelmien toimintojen jatkuvuudessa ja suojauksessa (Protection/Safety). Tässä opinnäytetyössä keskitytään juuri tähän osa-alueeseen.

5.4.2 Esineiden Internetin turvallisuus

Esineiden Internetin turvallisuus korostaa digitalisaatiota, manuaalisten toimintojen automatisointia, teollista ja esineiden Internetiä sekä niiden vaikutusta organisaation liiketoimintaan

ja tietoturvaan. Painotus on tietoturvakäytäntöjen muutoksissa suhteessa liiketoiminnan muutoksiin.

6 Kyberturvallisuus osana ohjaus-ja automaatiojärjestelmien elinkaarta

Vielä 1990-luvulla teollisuuden ohjaus- ja automaatiojärjestelmät olivat toimittajan suunnittelemia ja rakentamia sekä laitteistojen että sen sisältämien ohjelmistojen ja tietoliikenneprotokollien osalta. Järjestelmät olivat usein ns. suljettuja järjestelmiä (propriaty) eli ne eivät perustuneet yleisesti saatavilla oleviin tai standardoituihin teknisiin ratkaisuihin. Laitteistot, ohjelmistot ja tietoliikenneprotokollat olivat tiukasti sidoksissa keskenään eikä asiakkaalla/käyttäjällä ollut mahdollista vaikuttaa järjestelmän määriteltyyn tietoturvallisuustasoon. Asiakkaan kannalta järjestelmät oli ns. mustia laatikoita (black box), jotka suorittivat niille määriteltyjä toiminnallisia vaatimuksia (Weiss 2010, 1).

Nykyiset teollisuuden ohjaus- ja automaatiojärjestelmät pohjautuvat pitkälti standardoituihin teknisiin ratkaisuihin. Lisäksi järjestelmistä on tullut ns. kerroksellisia eli niistä on eroteltavissa käyttöjärjestelmä-, tietoliikenne- ja sovellustasot. Toiminnalliset vaatimukset määritellään sovellustasolla ja käyttöjärjestelmä tarjoaa sovellukselle rajapinnat laitteistolle ja kommunikointiin muiden teollisuuden ohjaus- ja automaatiojärjestelmien kanssa. Käyttöjärjestelmä- ja tietoliikenneratkaisut perustuvat yleisesti saatavilla oleviin ja standardoituihin teknisiin ratkaisuihin (Weiss 2010, 1).

Laitoksen ohjaus-ja automaatiojärjestelmät otetaan käyttöön yleensä pitkällä käyttöiän odotuksella (yli 20 vuotta). Merkittävät uudistukset, muutokset ja liiketoiminnan integraatiotarpeet edellyttävät kuitenkin, että sekä kehityksen että käytön aikana on useita ohjaus- ja automaatiojärjestelmiin liittyviä kehityshankkeita, joilla kaikilla voi olla turvallisuusvaikutuksia. Tämän vuoksi on välttämätöntä hallita ohjaus-ja automaatiojärjestelmien turvallisuutta koko elinkaaren ajan, joka usein koostuu neljästä keskeisestä vaiheesta:

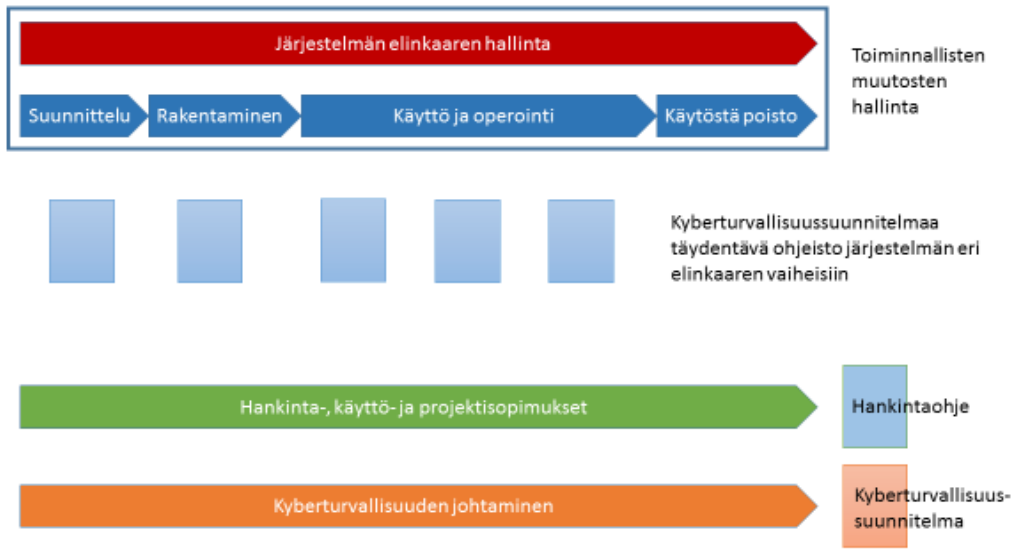
- suunnittelu
- rakentaminen
- käyttö ja operointi
- käytöstä poisto

Kaikki laitoksen ohjaus-ja automaatiojärjestelmiin liittyvät hankkeet tai toiminnot olisi suunniteltava siten, että turvallisuusnäkökohdat tulisi huomioiduiksi jo mahdollisimman varhaisessa vaiheessa. Tietoturvavaatimusten noudattamista ja implementointia olisi arvioitava säännöllisesti koko ohjaus- ja automaatiojärjestelmän elinkaaren ajan. Turvallisuusvaatimukset tulee olla sisällytetty osaksi hankinta-, suunnittelu- ja rakentamisprosessia. Laitoksen ohjaus- ja automaatiojärjestelmien käyttö- ja operointivaiheen tulee ylläpitää, toteuttaa ja noudat-

taa suunnitellut turvallisuusratkaisut ja -prosessit järjestelmän koko käyttöiän ajan (CPNI 2015).

Turvallisuustoimenpiteiden toteuttaminen laitoksen ohjaus- ja automaatiojärjestelmiin voi olla vaikeampaa ja kalliimpaa, kun järjestelmät on jo rakennettu ja otettu käyttöön. Tämän takia turvallisuustoimenpiteiden toteuttaminen elinkaaren alkuvaiheissa on aina tehokkaampaa, edullisempaa ja voi toimia jopa jonkin uuden liiketoimintamallin mahdollistajana.

Seuraavassa kuvassa on esitetty teollisuuden ohjaus- ja automaatiojärjestelmän elinkaari eri vaiheineen. Kuvaan on merkitty myös keskeisimmät tietoturvatoiminnot ja kyberturvallisuussuunnitelman ohjeet.



Kuva 3: Teollisuuden ohjaus- ja automaatiojärjestelmien elinkaari ja kyberturvallisuus

7 Kyberturvallisuussuunnitelma

Kyberturvallisuussuunnitelman tarkoitus on määrittää hallinnollinen prosessi, jonka tehtävänä on arvioida ja parantaa järjestelmällisesti tuotantolaitoksen käytössä olevien teollisuuden ohjaus- ja automaatiojärjestelmien ja niiden käyttämien tietoverkkojen turvallisuutta ja luotettavuutta. Teollisuuden ohjaus- ja automaatiojärjestelmillä on keskeinen rooli laitoksen tuotantoprosessissa ja ne vaikuttavat laitoksen tuottavuuteen, kustannustehokkuuteen ja työturvallisuuteen. Järjestelmien luotettavuuteen, kyberturvallisuuteen ja työturvallisuuteen liittyviä ominaisuuksia ei voida siten jättää ilman asianmukaista suunnittelua ja arviointia.

7.1 Suunnitelman yleisesittely

Suunnitelma kattaa kaikki tärkeimmät osa-alueet, joilla on vaikutusta teollisuuden ohjaus- ja automaatiojärjestelmien kyberturvallisuuteen, luotettavuuteen sekä järjestelmien toiminnollisuuteen. Suunnitelma ei kata pelkästään järjestelmien tekniset ominaisuudet, vaan myös käyttöhenkilöstön toiminnan (työntekijät ja kolmannen osapuolen henkilöstö), jotka ovat päivittäisessä vuorovaikutuksessa teollisuuden ohjaus- ja automaatiojärjestelmien kanssa. Lisäksi henkilöstö, jotka suunnittelevat, hankkivat ja ottavat käyttöön tällaisia järjestelmiä ovat suunnitelman vaikutuspiirissä (Suomen Automaatioseura ry 2005, 27).

Suunnitelma sisältää toimintoja, jotka on ryhmitelty neljään pääryhmään:

- Arkkitehtuurianalyysi
- Ihmiset ja menettelytavat
- Arviointi ja jatkuva parantaminen
- Johtaminen ja päätöksenteko

Suunnitelman toiminnot, jotka on kuvattu osiossa Arkkitehtuurianalyysi sekä Ihmiset ja menettelytavat, sisältävät suunnitelman suoritusosan. Toiminnot, jotka on kuvattu osiossa Arviointi ja jatkuva parantaminen, sisältävät menetelmät vaatimustenmukaisuuden ja suorituskyvyn arvioinneille ja kyberturvallisuussuunnitelman kehittämiselle. Arviointi ja jatkuva parantaminen -osiossa kuvattujen toimintojen tarkoitus on varmistaa, että kaikki suunnitelmassa määritellyt eri ryhmien toiminnot suoritetaan käytännössä. Johtaminen ja päätöksenteko -osio linkittää suunnitelman tuotantolaitoksen johtamisjärjestelmään. Tässä ryhmässä määriteltyjen toimintojen tarkoitus on varmistaa suunnitelman ohjaus ja valvonta, edistymisen arviointi ja kustannustehokkuus. Suunnitelmaan liittyvä raportointi ja johdon katselmointi suoritetaan määräajoin kerran vuodessa.

Seuraavassa kuvassa on esitetty suunnitelmassa mainittujen pääryhmien ja niissä määriteltyjen toimintojen välistä suhdetta. Lisäksi kuvaan on merkitty suunnitelmaa tarkentavat ja täydentävät ohjeistot, joita ei käsitellä yksityiskohtaisesti tässä opinnäytetyössä.

Kuva 4: Kyberturvallisuussuunnitelma ohjeistoineen

7.2 Suunnitelman soveltamisala

Tämän suunnitelman vaikutuspiirissä ovat tuotantolaitoksen teollisuuden ohjaus- ja automaatiojärjestelmät sekä näiden kanssa vuorovaikutuksessa olevat ihmiset ja laitoksen muut tietojärjestelmät.

7.3 Suunnitelmassa käytetyt keskeiset käsitteet ja lyhenteet

Teollisuuden ohjaus- ja automaatiojärjestelmiin liittyy paljon teknisiä käsitteitä ja lyhenteitä. Seuraavassa on kuvattu yleisellä tasolla suunnitelmassa käytetyt keskeiset käsitteet ja lyhenteet (Weiss 2010, 7).

7.3.1 Teollisuuden ohjaus- ja automaatiojärjestelmät

Teollisuuden ohjaus- ja automaatiojärjestelmillä tarkoitetaan kaikkia sellaisia digitaalisia laitteita, jotka on liitetty prosessiverkkoon tai niillä on muuten vaikutusta fyysiseen tuotantoprosessiin. Esimerkkejä em. laitteista voivat olla mm. turvajärjestelmät, operaattoripaneelit, järjestelmän ylläpitotyöasemat, SCADA-työasemat ja -palvelimet, älykkäät kenttälaitteet (ohjelmoitavat anturit, venttiiliohjaimet, ohjelmoitavat suojareleet ja ohjelmoitava taajuusmuuntajat), hajautetut ohjausjärjestelmät, historiapalvelimet, verkkolaitteet ja henkilökohtaiset työasemat.

7.3.2 Prosessiverkko

Prosessiverkolla tarkoitetaan tietoliikenneverkkoa, johon on liitetty yksi tai useampi teollisuuden ohjaus- ja automaatiojärjestelmä ja/tai muu digitaalinen järjestelmä, joita tarvitaan varmistamaan teollisen prosessin asianmukainen toiminta. Käytettävä verkkotekniikka ei rajoitu pelkästään TCP/IP -pohjaisiin tietoliikenneverkkoihin ja voi siten sisältää ei-IP -pohjaisia verkkoja (kuten H1, Profinet IRT, EtherCAT), kenttäväyliä, point-to-point -verkkoja sekä langattomia verkkoja.

7.3.3 Verkkoalue

Verkkoalueella tarkoitetaan sitä osaa prosessiverkkoa, joka on tavoitettavissa myös kyseisen verkkoalueen ulkopuolelta turvallisen mekanismin välityksellä. Em. mekanismin on suoritettava liikenteen suodatus ja raportointi oli valittu tekninen toteutustapa sitten mikä tahansa.

7.3.4 Verkkolaite

Verkkolaite on fyysinen laite, joka liitetään tietoliikenneverkkoon. Nämä pitävät sisällään sekä verkon aktiivilaitteet (esim. reitittimet, palomuurit, ja verkko-kytkimet) ja päätelaitteet (esim. ohjelmoitavat logiikat, etäpäätteet ja tietokoneet). "Liitetty verkkoon" ei tarkoita ainoastaan verkkoon pysyvästi liitettyjä järjestelmiä, vaan sisältävät myös liikuteltavat järjestelmät (esim. kannettava järjestelmän ylläpitotyöasemat ja langattomat yhteydet).

7.3.5 Digitaalinen laite

Laite on digitaalinen, mikäli se täyttää jonkun ao. määritelmistä:

- laitteen toiminta perustuu digitaaliseen koodiin, joka suoritetaan järjestelmän muistissa ("ohjelmoitavissa")
- laitteen toiminta perustuu asetusparametreihin, jotka on tallennettu digitaalisessa muodossa (esim. asetustiedosto)
- laite vastaanottaa tietoa digitaalisen liitännän kautta (esim. kenttäväylä, sarjayhteys, TCP/IP)
- laitteen käyttämät tiedot ovat tallennetut liikuteltavalla medialla (esim. USB, EPROM, tai levyke)

7.3.6 Tietokone

Tietokone on laitteisto, joka tukee kaikkia suosittuja käyttöjärjestelmiä (esim. Windows, Linux, Unix, MacOS).

7.4 Arkkitehtuurianalyysi

Tässä kappaleessa kuvataan suunnitelman edellyttämät vaatimukset tuotantolaitoksen järjestelmäinventaariolle, verkkoarkkitehtuurille ja tietovuokaavioille sekä järjestelmäsuunnittelulle ja -hankinnalle (Suomen Automaatioseura ry 2005, 67).

7.4.1 Järjestelmäinventaario

Tuotantolaitos ylläpitää inventaariota kaikista sen käytössä olevista teollisuuden ohjaus ja -automaatiojärjestelmistä ja tietoliikenneverkoista sekä muista tietojärjestelmistä, joilla on vaikutusta laitoksen tuotantoprosessien ohjaukseen ja valvontaan.

Järjestelmäinventaarion tarkoitus on:

- luoda perusta laitoksen verkkoarkkitehtuurille ja tietovuokaavioille
- tunnistaa ympäristöön kuulumattomat laitteet
- varmistaa laitteiden oikeat tai alkuperäiset asetustiedot
- varmistaa tiedot laitteiden identiteeteistä, sijainneista sekä muista erityispiirteistä, kuten käytössä olevista ohjelmistoversiosta, etäkäytöistä ja toimittajista
- tarjota dokumentaatio tarkemmalle haavoittuvuusanalyysille

Järjestelmäinventaario sisältää tiedot kaikista laitoksella käytössä olevista laitteista ja ohjelmistoista ja näiden asetustiedoista. Näiden tietojen avulla voidaan tarvittaessa varmistaa laitteiden ja ohjelmistojen asetustietojen oikeellisuus.

Käytössä olevista laitteista on kirjattu seuraavat tiedot järjestelmäinventaarioon:

- lyhyt järjestelmä/komponenttikuvaus
- tiedot laitteen valmistajasta, kapasiteetista ja käyttötarkoituksesta
- tiedot mahdollisesta verkkoliitynnästä (IP osoite, verkkoalue, käytössä olevista verkkopalvelut, levyjaot)
- tiedot käyttöjärjestelmäversiosta ja asennetuista ohjelmistoista
- laitteen sarjanumero

Käytössä olevista ohjelmistoista on kirjattu seuraavat tiedot järjestelmäinventaarioon:

- tiedot toimittajasta
- versiotiedot
- tiedot siitä, missä laitteissa kyseinen ohjelmisto on käytössä

Muutoshallinnan avulla varmistetaan se, että laitoksen järjestelmiin tehtävät muutokset, kuten nykyisten laitteistojen/ohjelmistojen uusinnat/vaihdot, uusien laitteiden/ohjelmistojen

asennukset sekä uusien ohjelmistoversioiden ja tietoturvakorjauksien asennukset tulevat kirjatuiksi järjestelmäinventaarioon tapahtumaperusteisesti.

Järjestelmäinventaario toteutetaan tietokantapohjaisella ohjelmistolla, joka mahdollistaa useamman samanaikaisen käyttäjän ja tapahtumakirjauksen. Vuosittaisilla katselmuksilla varmistetaan järjestelmäinventaarion tietojen oikeellisuus. Mahdolliset puutteet dokumentoidaan ja käsitellään seuraavassa vuosikatselmuksessa.

7.4.2 Verkkoarkkitehtuuri ja tietovuokaaviot

Tuotantolaitos ylläpitää prosessiverkon verkkoarkkitehtuuri- ja tietovuokaaviokuvauksia.

Verkko- ja tietovuokaaviokuvausten tarkoitus on kuvata tietojenvaihto ja riippuvuussuhteen laitoksen eri järjestelmien ja/tai laitteiden/komponenttien välillä.

Verkkokaaviot sisältävät kuvaukset:

- verkkojen eriyttämisestä ml. tiedot käytetystä liikenteen suodatusmekanismista (esim. reititin, palomuuri, kytkin tai mediamuunnin) sekä näiden toiminnollisuuksista
- loogisista IP verkoista
- langattomista verkoista ml. tiedot tukiasemien asetustiedoista
- tiedot mahdollisista etäyhteyksistä

Tietovuokaaviot sisältävät kuvaukset ohjelmistojen ja järjestelmien (ml. laitteet ja komponentit) rajapinnoista, toiminnollisuuksista sekä tiedot niistä ohjelmistoista ja järjestelmistä (ml. laitteet ja komponentit), joiden kanssa välittävät tietoa.

Muutoshallinnan avulla varmistetaan se, että kaikki verkkoon liittyvät muutokset, kuten esim. uusien järjestelmien asentaminen, sääntömuutos palomuureissa ja uusien etäyhteyksien luonti tulevat dokumentoitua laitoksen verkko- ja tietovuokaavioihin tapahtumaperusteisesti.

Verkkokaaviot sisältävät myös verkon päätelaitteet, joten ne tarjoavat täydellisen luettelon kaikista prosessiverkkoon kytketyistä järjestelmistä ja laitteista/komponenteista (ml. yhdyskäytävät muihin verkkoihin). Tietovuokaaviot esitetään graafisessa muodossa. Ne sisältävät tiedot käytettyjen ohjelmistojen rajapinnoista ja toiminnollisuuksista. Tietovuokaaviot eivät rajoitu ainoastaan IP-pohjaisiin verkkoihin, vaan sisältävät tiedot kaikista digitaalisista yhteyksistä kuten esim. sarjayhteyksistä ja kenttäväylistä. Kaikista valmistajan itse kehittämistä protokollista pyydetään tietovuokuvaukset ja liitetään viitteenä tietovuokaavioon.

Vuosittaisilla katselmuksilla varmistetaan verkko- ja tietovuokaavioiden oikeellisuus ja ajantasaisuus. Mahdolliset puutteet dokumentoidaan ja käsitellään aina seuraavassa katselmuksessa.

7.4.3 Järjestelmäsuunnittelu ja -hankinta

Tuotantolaitos sisällyttää kyberturvallisuus- ja luotettavuusnäkökulmat teollisuuden ohjaus- ja automaatiojärjestelmien suunnittelu- ja hankintaohjeistoja.

Tuotantolaitos määrittelee ja ylläpitää vakioituja kyberturvallisuus- ja luotettavuusvaatimuksia järjestelmätoimittajille lähetetyissä tarjouspyynnöissä ja järjestelmien hankintaehdoissa. Tavoitteena on, että laitoksen käyttämät teollisuuden ohjaus- ja automaatiojärjestelmätoimittajat täyttävät laitoksen kyberturvallisuus- ja luotettavuusvaatimukset. Jos jokin järjestelmätoimittaja ei täytä em. vaatimuksia, laitos pyrkii hankkimaan järjestelmät toiselta toimittajalta. Tuotantolaitos käyttää laitoksen virallista ohjeistoa ohjaus- ja automaatiojärjestelmien asennusten suunnittelussa sekä tehtäessä ennalta suunniteltuja järjestelmämuutoksissa, kuten verkkomuutokset ja -uusinnat sekä tehtäessä muita toiminnallisia tai arkkitehtonisia parannuksia.

Hankintaohjeiston tarkoitus on varmistaa, että uusien ohjaus- ja automaatiojärjestelmien hankinta ja asennus eivät heikennä laitoksen nykyistä kyberturvallisuus- ja luotettavuustasoa. Ohjeistoa käyttämällä voidaan varmistaa ja valvoa, että uusien ohjaus- ja automaatiojärjestelmien suunnittelu ja järjestelmiin liittyvien komponenttien (laitteet ja ohjelmistot) laatu täyttävät laitoksen nykyiset kyberturvallisuus- ja luotettavuusvaatimukset. Järjestelmäsuunnitteluun liittyvän ohjeiston tarkoitus on tarjota johdonmukaiset mallit ja menetelmät teollisuuden ohjaus- ja automaatiojärjestelmien suunnitteluun ja asennukseen, jotta varmistetaan laitoksen nykyiset kyberturvallisuus- ja luotettavuusvaatimukset (MSB 2014, 42).

Hankintaohjeisto sisältää vaatimukset:

- teknisten asiakirjojen sisällöstä ja laadusta (esim. tekniset yksityiskohdat käytetyistä verkkoprotokolleista ja -palveluista, tiedot suositeltavista varmistusmenetelmästä ja palomuuriavauksista)
- asennuksen eheyden varmistamisesta (esim. järjestelmän ns. koventaminen, tarpeettomien ja luvattomien ohjelmistojen poisto, versionhallinta, asetusten eheyden tarkistus)
- digitaalisten liityntöjen kyvystä sietää haitallista tai ennalta määrittämätöntä tietoliikennettä/tietoa
- käyttäjien pääsynhallinnasta ja käyttöoikeuksien hallinnasta
- toimittajan kyberturvallisuuteen liittyvistä prosesseista ja menettelytavoista

Järjestelmien suunnitteluohjeisto sisältää vaatimukset:

- prosessiverkkojen topologia- ja arkkitehtuurikuvauksista, käytetyistä IP-verkkojen osoitteistoista ja aliverkkoista, käytetyistä verkkoalueista ja -vyöhykkeistä (erityisesti toimistoverkot ja Internet), etäkäytöstä (erityisesti prosessiverkon hallintatyöasema), etäyhteyksistä (erityisesti toimistoverkosta ja/tai Internetistä) ja langattoman verkon tukiasemista
- keskeisten verkkoinfrastruktuuripalveluiden kokoonpanosta ja asetuksista, kuten DHCP (IP-osoitteiden jakaminen verkkoon kytkeytyville tietokoneille), NTP (aikatiedon välittäminen verkkoon kytkeytyneille tietokoneille), käyttäjätietokanta ja hakemistopalvelu (Active Directory) ja varmuuskopiointi
- verkkolaiteiden suojausasetuksista luvattoman pääsyn estämiseksi
- päätelaitteiden suojausasetuksista luvattoman pääsyn ja luvattomien ohjelmistojen asentamisen estämiseksi
- ohjeistosta eristää turvattomat järjestelmät (toimittajan patentoimat "mustat laatikot") prosessiverkosta

Laitoksen järjestelmäsuunnittelu- ja hankintaohjeistoa päivitetään vuosittaisen tehokkuusarvioinnin perusteella. Johdon hyväksyttyä ohjeistoon liittyvät muutokset, ohjeiston käyttäjiä on tiedotettava muutoksista. Tarvittaessa tulee järjestää koulutusta.

Järjestelmien hankintaohjeisto on kirjoitettava siten, että se sallii objektiivisen arvioinnin kyberturvallisuuteen liittyvän yksittäisen vaatimuksen täyttymisestä tai sen puutteesta. Vaatimusten täytyy mahdollistaa eri toimittajien samankaltaisten tuotteiden vertailun. Päätös siitä, että täyttyykö yksittäinen kyberturvallisuusvaatimus, ei saa perustua vapaamuotoiseen dokumentointiin, jonka tulkinnasta saattaisi syntyä erimielisyyttä kyberturvallisuusasiantuntijoiden kesken. Hankintaohjeistossa määriteltyjen järjestelmien kyberturvallisuusvaatimusten arviointitulokset säilytetään keskitetyssä järjestelmässä. Tämä sallii helpon ja nopean pääsyn eri järjestelmien ja toimittajien kyberturvallisuusominaisuuksiin ja -kyvykkyyksiin ilman uudelleenarviointeja.

Laitoksen järjestelmäsuunnittelu- ja hankintaohjeiston noudattamista seurataan muutoshallinnan avulla. Esimerkiksi ohjeiston katselmointi on osa järjestelmien FAT- ja SAT-testejä (Factory/Site Acceptance Tests). Niille teollisuuden ohjaus- ja automaatiojärjestelmille, joille FAT- ja/tai SAT-hyväksymistestausta ei suoriteta, tehdään pistokokeita vaatimustenmukaisuuden seuraamiseksi. Testauksen tulokset dokumentoidaan ja tiivistetään osaksi kyberturvallisuussuunnitelman vuosiraporttia.

7.5 Ihmiset ja menettelytavat

Tässä kappaleessa kuvataan suunnitelman edellyttämät vaatimukset tuotantolaitoksen käyttäjätietokannalle, koulutusohjelmalle sekä käyttöohjeille ja standardeille menettelytavoille (Suomen Automaatioseura ry 2005, 67).

7.5.1 Käyttäjätietokanta

Tuotantolaitos ylläpitää tietokantaa käyttäjistä, joilla on luvallinen pääsy laitoksen teollisuuden ohjaus- ja automaatiojärjestelmiin (ml. muut järjestelmät, jotka välittömästi vaikuttavat laitoksen tuotantoprosessiin). Käyttäjätietokannan tarkoitus on varmistaa käytännöllinen ja luotettava tapa laitoksen ohjeistojen ja menettelytapojen jakeluun ja käyttöönottoon sekä koulutusvaatimusten viestintään laitoksen työntekijöille.

Käyttäjätietokanta sisältää perustiedot kaikista niistä käyttäjistä, joilla on luvallinen pääsy laitoksen teollisuuden ohjaus- ja automaatiojärjestelmiin. Käyttäjät voivat olla laitoksen henkilökuntaa, järjestelmätoimittajia, urakoitsijoita ja/tai alihankkijoita. Tietokanta sisältää tiedot myös käyttäjien käyttöoikeuksista, rooleista ja vastuista eri järjestelmissä sekä tiedot suoritetusta koulutuksesta (laitoksen ohjeistot ja menettelytavat).

Muutoshallintaprosessin avulla varmistetaan käyttäjätietokantaan liittyvät päivitykset, mikäli käyttäjän työsuhde (henkilöstö) tai toimeksianto (järjestelmätoimittaja, urakoitsija ja alihankkija) laitoksella loppuvat, käyttäjän roolissa ja/tai vastuissa tapahtuu muutoksia tai uusille käyttäjille annetaan pääsy laitoksen teollisuuden ohjaus- ja automaatiojärjestelmiin. Muutoshallintaprosessi liittyy myös tilanteisiin, jossa laitoksen ohjeistoon ja menettelytapoihin tai koulutusvaatimuksiin tulee muutoksia.

Käyttäjätietokanta toteutetaan tietokantapohjaisella ohjelmistolla, joka mahdollistaa useamman samanaikaisen käyttäjän ja tapahtumakirjauksen. Vuosittaisilla katselmuksilla varmistetaan käyttäjätietokannan oikeellisuus ja ajantasaisuus. Mahdolliset puutteet dokumentoidaan ja käsitellään seuraavassa vuositarkastuksessa.

7.5.2 Koulutusohjelma

Tuotantolaitos ylläpitää koulutusohjelmaa, jotta kaikki laitoksella työskentelevät henkilöt voivat asiantuntevasti suorittaa Kyberturvallisuussuunnitelman edellyttämiä toimenpiteitä. Koulutusohjelman tarkoitus on varmistaa teollisuuden ohjaus- ja automaatiojärjestelmien kanssa välittömästi tai välillisesti työskentelevän henkilöstön (ml. järjestelmätoimittajat,

urakoitsijat ja alihankkijat) riittävä osaaminen, jotta he pystyvät suoriutumaan vastuullaan olevista tehtävistä laitoksen ohjeistojen ja menettelytapojen mukaisesti.

Koulutusohjelma kattaa kaikki Kyberturvallisuussuunnitelmassa mainitut osa-alueet ja toiminnot. Koulutusohjelman sisältö perustuu eri henkilöstöryhmien vallitsevaan kyberturvallisuustietämyksen ja -osaamisen.

Muutoshallintaprosessin avulla varmistetaan se, että laitoksessa käytössä olevaan teknologiaan, tuotteisiin sekä ohjeistoon ja menettelytapoihin liittyvät muutokset tulevat huomioitua myös koulutusohjelman sisällössä.

Koulutusohjelma on vakioitu ja modulaarinen. Laitoksen tavoitteena on tarjota yhtenäinen ja roolipohjainen koulutus henkilöstölle (ml. järjestelemätoimittajat, urakoitsijat ja alihankkijat), joilla on luvallinen pääsy laitoksen teollisuuden ohjaus- ja automaatiojärjestelmiin. Selainpohjaiset koulutusohjelmistot, jotka perustuvat itseopiskeluun ovat kustannustehokkuuden vuoksi suositeltavin vaihtoehto.

Vuosittaisilla katselmuksilla arvioidaan laitoksen teollisuuden ohjaus- ja automaatiojärjestelmien käyttäjien suorittamat koulutussuoritukset.

7.5.3 Käyttöohjeet ja standardit menettelytavat

Tuotantolaitos ylläpitää roolipohjaista tietovarastoa laitoksen teollisuuden ohjaus- ja automaatiojärjestelmiin liittyvistä käyttöohjeista ja standardeista menettelytavoista. Käyttöohjeiden tarkoitus on määrätä pakolliset tai kielletyt toimenpiteet, kun työskennellään Kyberturvallisuussuunnitelman alaisten järjestelmien parissa. Standardien menettelytapojen tarkoitus on kuvata yksityiskohtaisesti, kuinka kyberturvallisuussuunnitelman alaisiin järjestelmiin tehdään toistuvia toimenpiteitä vaarantamatta kuitenkaan laitoksen turvallisuutta ja luotettavuutta. Tietovarasto toimii keskitettynä järjestelmänä, josta on aina saatavilla kulloinkin voimassa olevat laitoksen käyttöohjeet ja menettelytavat.

Käyttöohjeet ja menettelytavat ovat saatavilla käyttäjärooleittain. Käyttäjän tarvitsee tutustua ainoastaan niihin ohjeisiin ja menettelytapoihin, jotka on tarkoitettu käyttäjän edustamalle roolille.

Keskeiset käyttäjäroolit sisältävät:

- Järjestelmätoimittajat, urakoitsijat ja alihankkijat
- Teollisuuden ohjaus- ja automaatiojärjestelmien ylläpitäjät
- Käyttöhenkilöstö (operaattorit)

- Järjestelmäsuunnittelijat

Keskeiset käyttötapaukset (käyttöohjeet ja standardit menettelytavat) sisältävät kuvaukset:

- Mobiililaitteiden käytöstä
- Etäkäyttöön liittyvistä menettelyistä
- Liikuteltavien muistimedioiden (mm. CD/DVD, USB-muistitikku ja -kovalevy) käytöstä
- Luvattomien ohjelmiston käytön estosta (mm. virustorjunta, tietoturvapäivitykset, järjestelmäkovennus)
- Tiedostojen siirrosta prosessiverkon ja muiden verkkojen välillä
- Verkon ja päätelaitteiden tietoturvan ylläpidosta

Käyttöohjeet ja standardit menettelytavat ovat muutoshallintaprosessin piirissä. Uudet tai päivitetyt ohjeet ja menettelytavat voidaan ottaa käyttöön vuosittaisten katselmusten tulosten perusteella. Uudet ohjeluonnokset annetaan ensin kommentoitavaksi niille käyttäjärooleille, joita luonnos käytännössä koskee. Edellisen kommentointikierroksen jälkeen, uudet käyttöohjeet ja menettelytavat julkaistaan niille tarkoitettuun tietovarastoon. Julkaisuprosessi varmistaa sen, että uusien käyttöohjeiden ja menettelytapojen vaikutuspiirissä oleville käyttäjille ilmoitetaan asiasta, huomioiden myös käyttäjien mahdolliset koulutustarpeet. Käyttöohjeisiin ja standardeihin menettelytapoihin liittyvä tietovarasto toteutetaan käyttämällä asiakirjojen hallintajärjestelmää (ml. asiakirjojen versiohallinta). Käyttöohjeet ja menettelytavat on kirjoitettu siten, että vaatimustenmukainen toiminta voidaan selkeästi ja yksiselitteisesti määritellä ja kuvata. Ilmaisuja kuten "mahdollisimman nopeasti" tai "tarvittaessa" ei käytetä. Menettelytapa, jolla varmistetaan se, että asiaankuuluvat osapuolet vastaanottavat ja ymmärtävät uudet käyttöohjeet ja standardit menettelytavat on määritelty (ml. koulutustarpeet) (ENISA 2011, 42).

Vuosittaisilla katselmuksilla arvioidaan sitä, onko laitoksen vallitseva toiminta käyttöohjeiden ja standardien menettelytapojen mukaista.

7.6 Arviointi ja jatkuva parantaminen

Tässä kappaleessa kuvataan suunnitelman edellyttämät vaatimukset tuotantolaitoksen kyberturvallisuustason arvioinnille, haavoittuvuusanalyysille ja suorituskyvyn arvioinnille (VTT 2010, 57).

7.6.1 Kyberturvallisuustason arviointi

Tuotantolaitos arvioi säännöllisesti sen kyberturvallisuuteen liittyviä valmiuksia. Tämä tarkoittaa käytännössä laitoksen Kyberturvallisuussuunnitelmassa määriteltyjen osa-alueiden ja

toimintojen kattavuuteen, paikkansapitävyyteen, yhdenmukaisuuteen tai niiden noudattamiseen liittyviä kokemusperäisiä arviointeja. Tätä tarkoitusta varten, laitos käyttää ja ylläpitää tosiasioihin perustuvaa mittaristoa. Laitoksen kyberturvallisuuteen liittyvien valmiuksien arvioinnin tarkoitus on tarkistaa se, kuinka perusteellisesti laitoksen Kyberturvallisuussuunnitelmassa määritellyt osa-alueet ja toiminnot on otettu käytännössä käyttöön.

Vuosittaisten katselmuksien tulosten perusteella, laitoksen kyberturvallisuusvalmiudet ilmaistaan:

- Järjestelmäinventaarion sisältämien tietojen kattavuudella ja paikkansapitävyydellä
- Verkkoarkkitehtuuri- ja tietovuokaaviokuvausten kattavuudella ja paikkansapitävyydellä
- Tuotantolaitoksen järjestelmäsuunnittelu- ja hankintaohjeistojen kattavuudella ja niiden noudattamisella
- Käyttäjätietokannan sisältämien tietojen kattavuudella ja paikkansapitävyydellä
- Koulutusohjelman kattavuudella ja sen noudattamisella
- Käyttöohjeiden ja standardien menettelytapojen kattavuudella ja niiden noudattamisella

Arvioinnissa käytettävää mittaristoa päivitetään arvioitaessa Kyberturvallisuussuunnitelman suorituskykyä (kappale 4.6.3). Eri ihmisten suorittamat arviointitulokset samasta osa-alueesta tai toiminnosta tulee olla yhteneväiset. Samoin arviointitulokset eri kyberturvallisuusominaisuuksilla varustetuista osa-alueista ja toiminnoista tulee olla eriävät. Laitoksen vuosittaisten kyberturvallisuusvalmiuksien arviointien tulokset tulee arvioida ja vahvistaa riippumattoman osapuolen toimesta vähintään joka kolmas (3) vuosi.

7.6.2 Haavoittuvuusanalyysi

Tuotantolaitos tekee järjestelmiin, arkkitehtuuriin sekä laitoksella käytössä oleviin käyttöohjeisiin ja menettelytapoihin liittyvän haavoittuvuusanalyysin. Analyysi ulottuu laite- ja komponenttitason haavoittuvuuksista koko laitostasoisiin haavoittuvuuksiin. Haavoittuvuusanalyysissä käytetään hyväksi järjestelmäinventaarion tietoja sekä verkkoarkkitehtuuri- ja tietovuokaaviokuvauksia. Haavoittuvuusanalyysin tarkoitus on tarjota tosiasiat päätöksenteon tueksi arvioitaessa tuotantolaitoksen vallitsevan kyberturvallisuustason riittävyyttä. Haavoittuvuusanalyysiä käytetään myös nykyisten järjestelmäasetusten, arkkitehtuurin ja menettelyohjeiden arviointiin laitoksen turvallisuuden takaamiseksi ja luotettavuuden varmistamiseksi (VTT 2010, 107).

Haavoittuvuusanalyysi sisältää tiedot:

- Nykyisistä tiedossa olevista haavoittuvuuksista

- Mahdollisesti jatkossa muodostuvista haavoittuvuuksista
- Mahdollisista seurauksista tai vaikutuksista
- Lakisääteisistä vaatimuksista ja muista lain edellyttämistä toimenpiteistä

Tieto äskettäin löydetystä haavoittuvuudesta, jolla saattaa olla vaikutus tuotantolaitoksen turvallisuuteen tai käytön luotettavuuteen komponentti-, laitos- tai prosessitasolla, käynnistää laitoksella muutokseen liittyvän prosessin. Haavoittuvuusanalyysi tehdään sillä olettamalla, että kohteen ympärillä olevat turvallisuusjärjestelyt ovat murtuneet. Haavoittuvuusanalyysi ei rajoitu pelkästään yksittäiseen komponenttiin, verkkoon kytkettyyn laitteeseen tai tietojärjestelmään, vaan sisältää kaikki digitaaliset laitteet ja niiden toiminnollisuuden. Haavoittuvuusanalyysin tulokset tule dokumentoida (Weiss 2010, 43).

Vuosittaisilla katselmuksilla varmistetaan se, että haavoittuvuusanalyysit on tehty ja asianmukaisesti dokumentoitu.

7.6.3 Suorituskyvyn arviointi

Tuotantolaitos arvioi Kyberturvallisuussuunnitelman tehokkuutta määriteltyyn kyberturvallisuus- ja luotettavuustasoon suhteutettuna, käsittäen myös lakisääteiset vaatimukset. Tehokkuuden arvioinnin tarkoitus on selvittää se, onko Kyberturvallisuussuunnitelman täytäntöönpano laitoksen edellyttämällä tai lakisääteisesti edellytetyllä kyberturvallisuus- ja luotettavuustasolla.

Suorituskyvyn arviointi sisältää:

- Analyysin kyberturvallisuuteen liittyvistä poikkeamista
- Arvion järjestelmäinventaarion tietojen tarkoituksenmukaisuudesta ja hyödyllisyydestä
- Arvion järjestelmien suunnittelu- ja hankintaohjeiston tarkoituksenmukaisuudesta ja hyödyllisyydestä
- Arvion koulutusohjelman tarkoituksenmukaisuudesta ja hyödyllisyydestä
- Arvion käytetystä mittaristosta kyberturvallisuusvalmiutta arvioitaessa
- Arvion haavoittuvuusanalyysin tarkoituksenmukaisuudesta ja hyödyllisyydestä
- Dokumentaation laitoksen nykyisen kyberturvallisuus- ja luotettavuustason lakisääteisestä riittävyydestä

Parannusehdotukset suorituskyvyn arviointiin tehdään tarkimmalla mahdollisella tavalla.

Koska tämän toiminnon tuotokset ovat olennaisia laitoksen johdon päätöksenteossa, ovat tulokset dokumentoitava johdon ymmärtämään muotoon eli teknisiä määritelmiä ja ilmaisuja on

vältettävä. Tuotantolaitoksen omista tarpeista tai mahdollisista lakisääteisistä vaatimuksista johtuen, suorituskyvyn arviointiin liittyvät tulokset voidaan arvioida ja vahvistaa riippumattoman osapuolen toimesta.

7.7 Johtaminen ja päätöksenteko

Arviointi ja jatkuva parantaminen -osa-alueen tulokset, parannustoimenpide-ehdotukset ja tämän edellyttämät resursointitarpeet (talousarvio) raportoidaan vuosittain laitoksen johdolle. Raportoinnin tarkoitus on antaa laitoksen johdolle selkeä kuva vallitsevasta kyberturvallisuustasosta, lakisääteisistä vaatimuksista, tietoa suunnitelman kustannustehokkuudesta ja maturiteetista, parannusehdotuksista sekä yksityiskohdista seuraavan vuoden talousarvion suunnitteluun. Päätöksenteon tarkoitus on varmistaa hallinnollinen perusta nykyisten tai päivitettyjen käyttöohjeiden ja standardien menettelytapojen täytäntöönpanosta sekä saada selkeä talousarviositoutuminen seuraavan vuoden kyberturvallisuussuunnittelulle ja sen edellyttämälle toteutukselle (Limnéll ym. 2014, 157; MSB 2014, 31).

Johdon raportti sisältää:

- Tarkemman kuvauksen laitoksen kyberturvallisuusvalmiuksista graafisessa esitysmuodossa ja keskeiset muutokset aikaisempiin raportteihin verrattuna ml. syyt muutoksille
- Yhteenvedon haavoittuvuusanalyyseistä ilman teknisiä yksityiskohtia sekä näihin liittyvät johtopäätökset ja suositukset
- Tulokset suunnitelman täytäntöönpanon tehokkuuden arvioinnista sisältäen laitoksen johdon hyväksynnän edellyttämät parannusehdotukset, kuten esim. päivitykset käyttöohjeisiin ja standardeihin menettelytapoihin
- Yhteenvedon suunnitelman toteutuneista kuluista ja arvion suunnitelman toteutuksen tehokkuudesta. Edellisten perusteella laitoksen johto päättää suunnitelman toteutuksen edellyttämästä talousarviosta seuraavalle vuodelle

Johdon hyväksyttyä raportin, Kyberturvallisuussuunnitelman parantamiseen liittyvät päätökset päivitetään suunnitelman eri osa-alueisiin ja toimintoihin. Tuotantolaitokselle osoitettu raportti on kirjoitettava mahdollisimman lyhyeksi ilman teknisiä ilmaisuja tai määritelmiä. Lisäksi johdon raportin tulisi sisältää arvion laitoksen kyberturvallisuusvalmiuksista verrattuna toimialaan yleensä.

Tuotantolaitoksen omista tarpeista tai mahdollisista lakisääteisistä vaatimuksista johtuen, raportointiin liittyvät sisällöt ja menetelmät voidaan arvioida ja vahvistaa riippumattoman osapuolen toimesta.

7.8 Roolit ja vastuut

Vastuu tuotantolaitoksen kyberturvallisuussuunnitelman edellyttämistä toimenpiteistä (johtaminen, suunnittelu ja toteutus) jakautuvat laitoksen eri yksiköille ja kolmansille osapuolille (järjestelmätoimittajat, urakoitsijat ja alihankkijat) (Suomen Automaatioseura ry 2005, 32).

7.8.1 Kyberturvallisuusyksikkö

Tuotantolaitoksen kyberturvallisuudesta vastaavan yksikön/osaston/tiimin/henkilön vastuulla on:

- Tarjota tekninen perusta järjestelmäinventaariolle ja vastata sen ylläpidosta
- Tarjota tekninen perusta käyttäjätietokannalla ja vastata sen ylläpidosta
- Luoda käyttöohjeet ja standardit menettelyohjeet sekä vastata niiden käyttöönotosta
- Luoda koulutusohjelma, kehittää sitä sekä järjestää ohjelman mukaisia koulutustilaisuuksia
- Suorittaa katselmointeja
- Suorittaa kyberturvallisuusvalmiuteen liittyviä arviointeja
- Suorittaa haavoittuvuusanalyyseja
- Suorittaa kyberturvallisuussuunnitelman toteutuksen tehokkuuteen liittyviä arviointeja
- Tukea käyttäjiä ja järjestelmien ylläpitäjiä sekä järjestelmätoimittajia, urakoitsijoita ja alihankkijoita Kyberturvallisuussuunnitelman edellyttämän täytäntöönpanon toteutuksessa

7.8.2 Henkilöstö ja muut yksiköt

Tuotantolaitoksen järjestelmäsuunnittelusta vastaavan yksikön/osaston/tiimin/henkilön on noudatettava laitoksen järjestelmäsuunnittelusta ja -hankinnasta annettuja ohjeita ja menetelmiä. Lisäksi heidän vastuullaan on arvioida se, kuinka hankintaohjeissa määritellyt kyberturvallisuusvaatimukset tulevat täytetyiksi teollisuuden ohjaus- ja automaatiojärjestelmien FAT- ja SAT-testien aikana. Arviointi voidaan suorittaa myös järjestelmien käyttöönottojen yhteydessä. Tällöin tulokset tulee raportoida laitoksen järjestelmäsuunnittelusta vastaavaan yksikköön/osastoon/tiimille/henkilölle.

Tuotantolaitoksen hankinnasta ja lakiasioista vastaavien yksiköiden/osastojen/tiimien/henkilöiden vastuulla on määritellä laitoksen hankintaohjeet, jotka sisältävät kyberturvallisuuteen ja palvelutasoon liittyvät vaatimukset sekä oikeudellisesti sitovat hankinta- ja palvelusopimukset.

Tuotantolaitoksen ylläpidosta vastaavan yksikön/osaston/tiimin/henkilön on noudatettava laitoksen järjestelmien ylläpitoon ja huoltoon liittyvä käyttöohjeita ja standardeja menettelytapoja. Lisäksi sen vastuullaan on muutoshallinta yhteydessä päivittää järjestelmäinventaarion sisältämiä tietoja järjestelmien käyttöönottojen, muutosten ja vaihtojen yhteydessä.

Tuotantolaitoksen operatiivisesta käytöstä vastaavan yksikön/osaston/tiimin/henkilön on noudatettava laitoksen järjestelmien käyttöön ja operointiin liittyviä käyttöohjeita ja standardeja menettelytapoja (erityisesti järjestelmien ja liikuteltavien muistimedioiden käytöstä annetut ohjeet).

Tuotantolaitoksen muiden yksiköiden käyttäjien (esim. tuotannonsuunnittelu ja laadunhallinta), jotka ovat yhteydessä laitoksen prosessiverkkoon, on noudatettava laitoksen järjestelmien etäkäyttöön liittyviä käyttöohjeita ja standardeja menettelytapoja (erityisesti sovellus- ja verkkomuutokset tulee hyväksyttää ensin laitoksen kyberturvallisuusyksikössä).

Tuotantolaitoksen tietotekniikasta/-hallinnosta (IT) vastaavan yksikön/osaston/tiimin/henkilön vastuulla on tukea laitoksen kyberturvallisuusyksikköä Kyberturvallisuussuunnitelman toteutuksen suorituskyvyn arvioinneissa vuosiraportoinnin perusteella. Lisäksi sen vastuulla on tarjota IT-tekninen perusta ja parhaat IT-käytännöt suunnitelman toteutuksen suorituskyvyn parantamiseksi.

7.8.3 Kolmannet osapuolet

Teollisuuden ohjaus- ja automaatiojärjestelmien toimittajat, urakoitsijat, alihankkijat sekä järjestelmä-integraattorit vastaavat siitä, että laitoksen:

- hankintaohjeissa mainitut kyberturvallisuusvaatimukset tulevat täytetyiksi järjestelmäkehityksen, FAT- (Factory Acceptance Testing) ja/tai SAT-hyväksymistestauksien (Site Acceptance Testing) tai käyttöönoton aikana
- järjestelmien ylläpitoon ja huoltoon liittyviä käyttöohjeita ja standardeja menettelytapoja noudatetaan (erityisesti etäkäyttö, mobiililaitteiden käyttö, liikuteltavien muistimedioiden käyttö sekä pääkäyttäjä-/järjestelmätason käyttö)

Tuotantolaitos voi erillisen toimeksiannon perusteella palkata ulkopuolisen asiantuntijan (konsultti) suorittamaan kybertuvallisuussuunnitelmaan määriteltyjä toimintoja. Erityisesti laitoksen vuosittaisen kyberturvallisuusvalmiuksien arviointiin ja vahvistamiseen sekä erilaisten mallien/menetelmien ja tietovarastojen parantamiseen voidaan käyttää ulkopuolista asiantuntijaa.

7.8.4 Johto

Tuotantolaitoksen johdon vastuulla on käsitellä ja hyväksyä laitoksen Kyberturvallisuussuunnitelman toteutukseen liittyvä vuosiraportti (kappale 4.7), käyttöohjeet ja standardit menettelytavat sekä suunnitelman ylläpidon ja toteutuksen edellyttämät resursoinnit (talousarvio).

8 Kyberturvallisuussuunnitelman ohjeisto

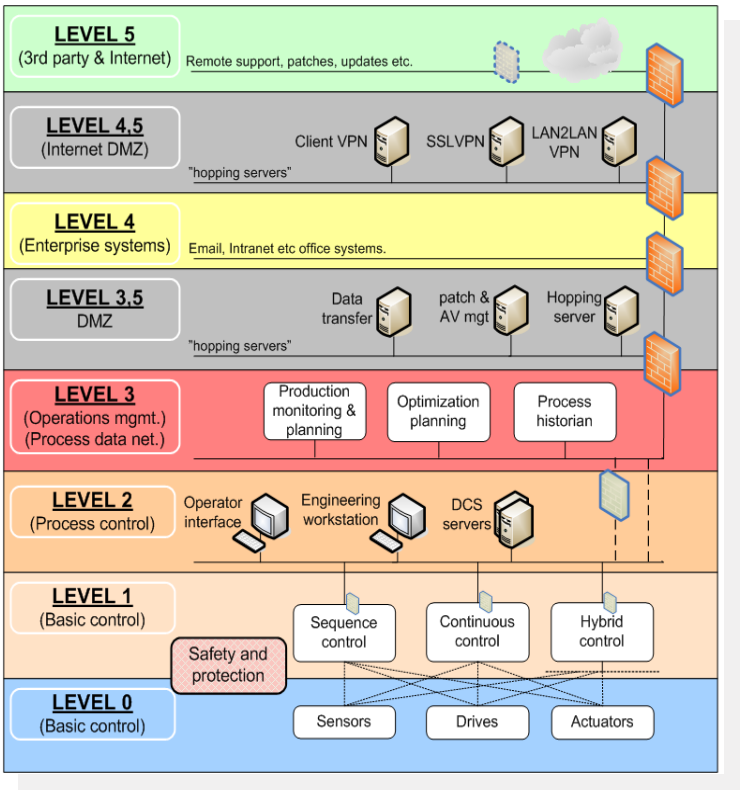
Seuraavassa esitellään kyberturvallisuussuunnitelmaan liittyvät ohjeistot ja tekniset vaatimusmäärittelyt. Niiden tarkoitus on tarkentaa suunnitelmassa mainittuja asiakokonaisuuksia. Samalla ne toimivat vaatimusmäärittelyinä esim. laitoksen ohjaus- ja automaatiojärjestelmiin liittyvissä hankinta-ja kehitysprojekteissa sekä esim. ulkoistettaessa laitoksen käyttö-ja operointitoimintoa kolmansille osapuolille. Ohjeistot on käsitelty ainoastaan johdanto-tasolla.

8.1 Järjestelmien suunnitteluohje

Ohje sisältää säännöt turvallisen ohjaus- ja automaatiojärjestelmän suunnittelulle ja toteutukselle (asennus ja konfigurointi). Ohjetta voidaan käyttää sekä arvioitaessa laitoksen laitteistojen, sovellusten ja verkkoinfrastruktuurin integrointia käytössä olevissa järjestelmissä ja/tai referenssinä suunniteltaessa uusia järjestelmiä tai niiden laajennuksia. Suunnitteluohje voidaan käsittää ns. vastinparina laitoksen käyttö- ja operointiohjeelle sillä tavalla, että käyttö- ja operointiohjeet määrittävät säännöt laitoksen ihmisten ja ohjaus- ja automaatiojärjestelmien vuorovaikutukselle (esim. kuinka kirjautua ulos päätelaitteilta tai miten käyttää USB-muistitikkuja), kun taas suunnitteluohje sisältää pysyvimpiä vaikutuksia (esim. määrittää tai muuttaa järjestelmän ominaisuuksia ja käyttäytymistä) (Langner 2012, 83).

Suunnitteluohjeen keskeisin kohta on laitoksen ohjaus-ja automaatiojärjestelmiin liittyvä tietoverkkoarkkitehtuuri. Tällä tarkoitetaan mm. eri toimintoja sisältävien tietoverkkosegmenttien suhdetta toisiinsa, tietoverkkojen kriittisyysluokittelu, eri tietoverkkosegmenttien välinen tietoliikenne ja pääsyä Internetistä eri tietoverkkosegmentteihin. Segmentoinnin perustarkoitus on saada aikaan puolustuksellista syvyyttä, jossa ylimmät/uloimmat verkkokerrokset suojaavat aina alempaa/sisempää verkkokerrosta. Kaikkein kriittisimmät toiminnot/palvelut ja niitä tuottavat ohjaus- ja automaatiojärjestelmät ovat sijoitettu aina alimpiin/sisimpiin verkkokerroksiin. Lisäksi verkkokerrosten välinen kommunikointi tulee määritellä sellaiseksi, että yhteyden muodostaminen voidaan aloittaa aina turvallisemmasta kerroksesta (Weiss 2010, 50-51).

Seuraavassa kuvassa on esitetty malli tietoverkkosegmenttirakenteesta, jossa kaikkein kriittisimpiä ohjaus- ja automaationtoimintoja sisältävät tietoverkkosegmentit sijaitsevat alimmilla vyöhykkeillä. Kuvassa on käytetty englanninkielisiä termejä.



Kuva 5: Teollisuuden ohjaus- ja automaatiojärjestelmien verkkoarkkitehtuuri

8.2 Järjestelmien hankintaohje

Ohje sisältää tuotantolaitoksen ohjaus- ja automaatiojärjestelmien kyberturvallisuuden peruskriteerit, joita käytetään joko tarjouspyynnön yhteydessä tai tuotekehityksen vaatimusmäärittelyssä. Kriteerit sisältävät vaatimuksia mm. järjestelmädokumentaatiolle (esim. verkko- ja tietovuokaaviot), muutostenhallinnalle, verkkoarkkitehtuurille (esim. verkon kerroksellisuus), pääsynhallinnalle sekä toimittajan prosesseille ja menettelyohjeille (esim. tietoturvapäivitysten asennus ja tietoturvapoikkeamien hallinta) (Weiss 2010, 223).

8.3 Ohje järjestelmien tietovuokaavioista

Ohjeessa määritellään menettelyt, joita käytetään tuotantolaitoksen ohjaus- ja automaatiojärjestelmien graafisissa tietovuokaavioissa. Kaaviolla kuvataan järjestelmäasennuksen eri komponenttien väliset digitaaliset vuorovaikutukset. Tietovuokaaviot eroavat tietoverkkokaavioista, koska tietoverkkokaaviot kuvaavat mahdolliset pääsyreitit järjestelmille, kun taas

tietovuokaaviot kuvaavat todelliset vuorovaikutusreitit ja riippuvuudet, jotka toteutetaan eri ohjelmistoissa, mukaan lukien käyttöjärjestelmät (Langner 2012, 59).

8.4 Ohje tietoverkkokaavioista

Tietoverkkokaaviot ovat olennainen osa tuotantolaitoksen ohjaus- ja automaatiojärjestelmien dokumentaatiota. Yleisesti hyväksyttyä standardia ei ole siitä, mitä tietoverkkokaavioissa pitäisi olla kuvattuna ja miten erilaiset järjestelmäkomponentit tulisi kuvata kaaviossa (Langner 2012, 59). Tämän ohjeen tavoitteena on varmistaa, että tietoverkkokaaviot ovat tehty johdonmukaisella tavalla ja sisältävät kaikki tarvittavat tiedot, joita tarvitaan verkkoarkkitehtuurin tarkoituksenmukaisuuden arvioimiseksi kyberturvallisuuden kannalta.

8.5 Järjestelmien käyttö- ja operointiohjeet

Tässä ohjeessa määritellään tietoturvalliset käyttö- ja operointiohjeet, jotka ohjaavat tuotantolaitoksen henkilöstön vuorovaikutusta laitoksen ohjaus- ja automaatiojärjestelmien kanssa. Tämä ohje täydentää järjestelmien suunnitteluohjetta, jossa esitetään säännöt turvallisten järjestelmien suunnitteluun ja toteutukseen (asennus ja konfigurointi). Käyttö- ja operointiohjeet ohjeistavat laitoksen ohjaus- ja automaatiojärjestelmien kanssa vuorovaikutuksessa olevien henkilöiden toimintaa (esim. ulos kirjautuminen käyttöpäätteiltä tai USB-tikkujen käyttäminen), kun taas suunnitteluohjeet määrittävät tietoverkkojen tai ohjelmistojen digitaalisia ominaisuuksia (MSB 2014, 44).

8.6 Ohje tietoturvapoikkeamien hallinnasta

Ohjeen tarkoitus on minimoida potentiaalisten ja todellisten tietoturvapoikkeamien kielteiset vaikutukset mahdollisimman tehokkaasti soveltamalla ennalta määrättyjä menettelytapoja, joita koordinoidaan ja suoritetaan toimivaltaisen ryhmän toimesta. Tässä yhteydessä tietoturvapoikkeamalla tarkoitetaan tuotantolaitoksen ohjaus- ja automaatiojärjestelmiä uhkaavaa tai tapahtunutta poikkeamaa joko järjestelmän toiminnassa tai sen käytössä. Tietoturvapoikkeamat eivät välttämättä ole tahallisia. Suurin osa todetuista tietoturvapoikkeamista ovat johtuneet vahingosta tai toimimalla tietämättään vastoin sovittuja käyttö- ja operointiohjeita. Satunnaista vikaantumista ei pidetä tietoturvapoikkeamana (Weiss 2010, 165).

8.7 Ohje järjestelmäinventaariosta

Järjestelmäinventaario on keskeinen tekijä tuotantolaitoksen ohjaus- ja automaatiojärjestelmien toiminnan varmistamisessa (järjestelmän suunnittelusta ja ylläpidosta) ja kyberturvallisuuden takaamisessa. Monissa ohjaus- ja automaatioympäristöissä järjestelmäinventaario on

usein puutteellista ja vanhentuneen laskentataulukon muodossa, jos sitäkään. Tällainen toiminta johtaa usein siihen, että ymmärrys laitoksen järjestelmistä ja niiden eri komponenteista on puutteellista ja tämä taas saattaa rajoittaa kyberturvallisuussuunnitelman toteutusta. Järjestelmäinventaario ei ole vain laitoksen ohjaus- ja automaatiojärjestelmiin liittyvä laitteisto- ja ohjelmistoluettelo. Se sisältää tietoa myös järjestelmien eri riippuvuuksista ja järjestelmiin tehdyistä muutoksista. Lisäksi järjestelmäinventaariolla on keskeinen merkitys laitoksen ohjaus- ja automaatiojärjestelmiin liittyvien tietoturvauhkien tunnistamisessa ja analysoinneissa (Langner 2012, 72-75).

8.8 Ohje järjestelmien käyttäjätietokannasta

Tuotantolaitoksen ohjaus- ja automaatiojärjestelmiin liittyvä käyttäjätietokantaa voidaan pitää laitoksen järjestelmäinventaariota täydentävänä. Käyttäjätietokanta keskittyy laitoksen henkilöihin ja näiden yhdistämiseen eri rooleihin ja vastuualueisiin sekä niihin liittyviin prosesseihin. Laitoksen järjestelmäinventaario taas keskittyy laitoksen teknisiin järjestelmiin ja näiden ominaisuuksiin, kuten käyttöjärjestelmäversioihin ja IP-osoitteisiin. Lisäksi käyttäjätietokannassa ylläpidetään tietoa laitoksen henkilöiden käyttöoikeuksista, yhteystiedoista ja koulutusvelvoitteista (Langner 2012, 76).

9 Kyberturvallisuussuunnitelman täytäntöönpano

Tuotantolaitoksen teollisuuden ohjaus- ja automaatiojärjestelmien luotettavuuden takaamiseksi ja turvallisuuden varmistamiseksi kehitetty kyberturvallisuussuunnitelma (prosessi) ei käynnisty itsestään, vaan vaatii laitokselta organisatorisia ja teknisiä edellytyksiä. Lisäksi kyberturvallisuussuunnitelman mukainen toiminta edellyttää laitokselta standardoituja kuvaustapoja ja työkaluja verkkoarkkitehtuurikuvausten ja tietovuokaavioiden luontiin ja esittämiseksi.

Kyberturvallisuussuunnitelman käyttöönotto kannattaa tehdä projektinluonteisesti, jossa tulee noudattaa laitoksen käytössä olevaa projektityömenetelmää. Tuotantolaitoksen koosta ja lukumäärästä riippuen, suunnitelman täytäntöönpanoon kuluu aikaa yhdestä (1) vuodesta kuuteen (6) vuoteen.

9.1 Organisaatio ja resursointi

Usein laitoksen ohjaus- ja automaatiojärjestelmiin liittyvät tietoturva-asiat nähdään toimenpiteinä, joita tehdään yksittäisen (automaatio)insinöörin toimesta muun työn ohessa. Lisäksi tietoturvaan liittyvien toimenpiteiden taustalla ei ole johdon hyväksymää suunnitelmaa ja/tai

resursointia. Edellä mainittua kuvausta voidaankin pitää monesti kyberturvallisuussuunnitelman täytäntöönpanon lähtötilanteena organisatoriselta kannalta katsottuna.

Kyberturvallisuussuunnitelman täytäntöönpanoon liittyvän projektisuunnitelman tulee sisältää projektiorganisaatio (roolit ja vastuut), tavoite, aikataulu, kohde (yksi tuotantolaitos, useita tuotantolaitoksia) sekä arvio vaadittavista resursseista (talousarvio), joita tarvitaan kyberturvallisuussuunnitelman käynnistämiseksi (mm. tietovarastot järjestelmäinventaariolle ja käyttäjille) ja kyberturvallisuussuunnitelmassa määritellyn prosessin "ensimmäisen kierroksen" suorittamiseksi (mm. ulkoisen asiantuntemuksen resursoinnin tarve) (MSB 2014, 31-35).

Projektin onnistumisen edellytyksenä on projektityhmän oikea kokoonpano. Projektiorganisaation tulee kuulua laitoksen johdon edustaja, kyberturvallisuudesta vastaava, IT:stä ja tietoverkoista vastaavat sekä laitoksen käytöstä ja ylläpidosta vastaavat henkilöt. Mikäli laitoksen oma tietoturvaosaaminen tai -resursointi on puutteellista, on ulkopuolisen tieto- tai kyberturvallisuusasiantuntijan nimeäminen projektiin olla myös perusteltua.

Projektisuunnitelma hyväksytetään laitoksen johdolla ja siitä tulee informoida myös laitoksen omia työntekijöitä sekä laitoksen toimintaan liittyviä kolmansia osapuolia (järjestelmä- ja palvelutoimittajat sekä urakoitsijat ja alihankkijat).

9.2 Tietovarastot järjestelmä- ja käyttäjätiedoista

Tyypillisesti tuotantolaitoksen teollisuuden ohjaus- ja automaatiojärjestelmien laitteisto-, sovellus- ja käyttäjätietoja ylläpidetään Excel-taulukoiden avulla. Useinkaan taustalla ei ole muodollista prosessia tai automatisointia tietojen ylläpitämiseksi, jolloin tietojen ajantasaisuus ja oikeellisuus ovat kyseenalaisia. Lisäksi em. tietojen paljastuminen ulkopuolisille tai niiden menettäminen esim. yksittäisen laitteistorikon vuoksi, saattavat vaarantaa tuotonlaitoksen toiminnan (huolto ja ylläpito).

Teollisuuden ohjaus- ja automaatiojärjestelmien turvallisuuden varmistamisen lähtökohtana tuleekin olla ajantasainen ja oikea tieto siitä, että mitä järjestelmiä laitoksella on käytössä ja keillä henkilöillä on käyttöoikeus em. järjestelmiin. Tämä edellyttää erillisen tietokantapohjaisen tietovaraston perustamista (tietokanta järjestelmäinventaariolle ja käyttäjätiedoille), jonka käyttöä voidaan kontrolloida eritasoisten käyttöoikeuksien perusteella. Tietovarasto voi perustua valmiiseen kaupalliseen ratkaisuun tai se voidaan tehdä laitoksen omista lähtökohdista räätälöitynä. Tietovarasto tulee olla kaikkien laitoksella työskentelevien henkilöiden käytettävissä ennalta määriteltyjen käyttöoikeuksien puitteissa. Käyttäjätietoja tallennettaessa ja käsiteltäessä on huomioitava henkilötietojen käsittelyyn liittyvät juridiset edellytykset, kuten esim. käyttötarkoitussidonnaisuus ja rekisteriselosteen luonti. Lisäksi tietovaraston

tulisi olla keskitetty, jotta sinne keskitetään tarvittaessa useamman laitoksen järjestelmäinventaario- ja käyttäjätiedot.

Tarkemmat kuvaukset järjestelmäinventaarioon ja käyttäjätietoihin liittyvistä tietokannoista, niiden sisällöistä ja liittymistä laitoksen muihin tietojärjestelmiin, automaattisesta tietojenkeruusta eri kohdejärjestelmistä ja näihin liittyvistä menetelmistä sekä tietokantojen käyttöoikeuksista tulee määritellä erillisillä kyberturvallisuussuunnitelmaan kuuluvilla ohjeistoilla. Näiden ohjeistojen sisältöä ei käsitellä tarkemmin tässä opinnäytetyössä.

9.3 Tietovarasto kyberturvallisuusohjeistolle

Kyberturvallisuussuunnitelman täytäntöönpanoprojektissa luodaan tuotantolaitoksen kyberturvallisuusohjeista, joka pitää sisällään menettelyohjeita ja teknisiä vaatimuksia. Ohjeisto ja vaatimukset muodostuvat seuraavista dokumenteista:

- Järjestelmien käyttö- ja operointiohjeet
- Järjestelmien hankintaohje
- Järjestelmien suunnitteluohje
- Ohje tietoturvapoikkeamien hallinnasta
- Ohje järjestelmien tietovuokaavioista
- Ohje järjestelmien tietoverkkokaavioista
- Ohje järjestelmien käyttäjätietokannasta
- Ohje järjestelmäinventaariosta

Edellä mainittujen kyberturvallisuusohjeistojen ja teknisten vaatimusmäärittelyjen sisällöt on käsitelty ainoastaan johdanto-tasolla tässä opinnäytetyössä.

Kyberturvallisuussuunnitelmasta ja sen sisältämistä menettelyohjeistoista ja teknisistä vaatimuksista muodostuu oma tietovarasto, jota tulee pystyä ylläpitämään keskitetysti ja sähköisesti. Tämä edellyttää sähköistä dokumenttienhallintamenetelmää (-järjestelmää). Ohjeistojen ja vaatimusten tulee olla laitoksen kaikkien käyttäjien käytössä ennalta määriteltyjen käyttöoikeuksien puitteissa. Dokumentteihin liittyvät muutosoikeudet tulee rajata ainoastaan laitoksen kyberturvallisuudesta vastaaville. Laitoksen muilla käyttäjillä on lähtökohtaisesti dokumentteihin ainoastaan lukuoikeudet. Käytössä oleva hallintamenetelmä (-järjestelmä) tulee tukea dokumenttien versiointia ja muutoslokia.

9.4 Muut työkalut ja tietovarastot

Tietovuokaavioiden avulla ymmärretään paremmin laitoksen ohjaus- ja automaatiojärjestelmien väliset riippuvuudet sekä hallitaan järjestelmien teknisten komponenttien liitynnät ja

rajapinnat sekä näihin liittyvät mahdolliset haavoittuvuudet. Tietovuokaavioiden kuvaamiseen ja esittämiseen käytetään standardoitua UML-mallinnuskieltä. Tarjolla on sekä kaupallisia (maksullisia) että avoimeen lähdekoodiin perustuvia (ilmaisia) UML-editoreita.

Teollisuuden ohjaus- ja automaatiojärjestelmiin liittyvät tietoverkkokaaviot ovat tärkeitä apuvälineitä laitoksen verkkoarkkitehtuurin ja siihen mahdollisesti liittyvän tietoverkon pääsynhallinnan ymmärtämisessä ja kuvaamisessa. Kattavien ja ajantasaisten verkkokaavioiden ylläpito on välttämätöntä laitoksen ohjaus- ja automaationjärjestelmien luotettavuuden takaamisessa ja turvallisuuden varmistamisessa. Verkkokaavioiden luontiin ja esittämiseen ei ole olemassa yleisesti hyväksyttyä tai standardoitua menetelmää. Verkkokaavioiden luontiin on tarjolla sekä kaupallisia (maksullisia) että avoimeen lähdekoodiin perustuvia (ilmaisia) työkaluja. Tuotantolaitos määrittää itse, millä työkalulla laitoksen ohjaus- ja automaatiojärjestelmiin liittyvät verkkokaaviot luodaan ja esitetään.

Tarkemmat kuvaukset UML-mallinnuskielen käytölle sekä verkkokaavioiden luontiin ja esittämiseen tulee määritellä erillisillä kyberturvallisuussuunnitelmaan kuuluvilla ohjeistolla. Näiden ohjeistojen sisältöä ei käsitellä tarkemmin tässä opinnäytetyössä, ainoastaan johdantotasolla.

Tuotantolaitoksen teollisuuden ohjaus- ja automaatiojärjestelmiin liittyvien tietovuo- ja verkkokaavioiden ylläpito ja säilytys tehdään tarkoitukseen varatussa tietovarastossa (tietokanta). Tarkemmat kuvaukset tietovuo- ja verkkokaavioihin liittyvästä tietokannasta ja sen sisällöstä tulee määritellä erillisillä kyberturvallisuussuunnitelmaan kuuluvalla ohjeistolla.

9.5 Suunnitelman käyttöönotto

Kun määritellyt organisatoriset ja tekniset edellytykset on laitoksella luotu sekä tarvittavat työkalut valittu, voidaan kyberturvallisuussuunnitelman mukainen toiminta laitoksella aloittaa. Kuten aikaisemmin on todettu, tuotantolaitoksen kyberturvallisuussuunnitelma sisältää ennalta määrättyjä toimenpiteitä, jotka seuraavat laitoksen vuotuista suunnittelu- ja johtamisjärjestelmiä. On kuitenkin huomattava, että kyberturvallisuussuunnitelmassa määritellyn prosessin "ensimmäisellä kierroksella" päivitetään ja käytännössä testataan laitoksen uusia kyberturvallisuussuunnitelmaan liittyviä ohjeistoja ja vaatimuksia. Tästä syystä prosessin ensimmäinen kierros vaatii enemmän työtä ja resursointia kuin seuraavien vuosien vastaavat kierrokset, joten ensimmäinen kierros kannattaa sisällyttää osaksi kyberturvallisuussuunnitelman käyttöönottoprojektia.

Arvioitaessa laitoksen kyberturvallisuustasoa ja kyberturvallisuussuunnitelman suorituskykyä ensimmäisen kierroksen jälkeen, on melko todennäköistä, että kehitettävää on laitoksen val-

litsevassa kyberturvallisuustasossa ja kyberturvallisuussuunnitelmaan liittyvien ohjeistojen ja vaatimusten sisällössä sekä itse suunnitelman toteuttamisessa. Koska kyberturvallisuussuunnitelman mukainen toiminta perustuu laitoksen kyberturvallisuuden jatkuvaan parantamiseen, on ensimmäisen kierroksen aikana havaitut poikkeamat ja puutteet sekä epäkohdat suunnitelman toteutuksessa huomioitava seuraavan vuoden suunnitelman toteutuksessa (mm. kehitystoimenpiteet ja niiden edellyttämä resursointi).

10 Yhteenveto ja johtopäätökset

Kesäkuussa 2010 havaittiin ensimmäinen kohdennettu haittaohjelma (Stuxnet), jolla pystyttiin vaikuttamaan teollisuuden ohjaus- ja automaatiojärjestelmän fyysiseen toimintaan (Langner 2013). Tämän jälkeen on mediassa raportoitu useista muistakin vastaavista tapauksista, joissa kohdennetun haittaohjelman avulla on voitu suoraan vaikuttaa tuotantoprosessiin ja/tai -ohjaukseen. Kohteina ovat olleet ainakin Saksalainen teräsyhtiö ja Ukrainalainen energiayhtiö. Yhteistä em. tapahtumilla on se, että sähköisellä/loogisella hyökkäyksellä saadaan aikaan reaalimaailmassa havaittava fyysinen seuraus (vahinko). Näissä tilanteissa vaikutukset saattavat aiheuttaa vaaraa joka ihmisten hengelle ja terveydelle. Tämänlaiset operaatiot vaativat hyökkääjältä todella paljon valmistelua, osaamista ja resursointia, jolloin potentiaalinen tekijätaho kaventuu valtiollisiin toimijoihin tai valtion rahoittamiin yksityisiin toimijoihin.

Opinnäytetyön tarkoituksena oli esitellä menetelmä teollisuuden ohjaus- ja automaatiojärjestelmiä käyttävän tuotantolaitoksen kyberturvallisuusasioiden kehittämiseksi ja johtamiseksi. Esitettävän menetelmän tarkoitus ei ole estää tai pysäyttää valtiollisten tahojen mahdolliset kyberhyökkäykset tuotantolaitoksen teollisuuden ohjaus- ja automaatiojärjestelmiä vastaan, vaan liittää kyberturvallisuusasiat osaksi laitoksen normaalia johtamisjärjestelmää. Tällä tavoin kyberturvallisuusasioita johdetaan ja niistä raportoidaan samalla tavoin kuin muistakin laitokselle tärkeistä asioista. Yksittäisistä raportoiduista kohdennetuista hyökkäyksistä huolimatta, merkittävä tekijä laitoksen tietoturvapoikkeamin syihin on oman henkilöstön väärä toimintamalli, joka johtuu taas asiaan kuuluvan koulutuksen tai ohjeiston puutteesta (ENISA 2011, 42).

Vaikka kyberturvallisuussuunnitelma on hyvin prosessikeskeinen ja perustuu jatkuvaan kehittämiseen (laitoksen koko elinkaaren ajan), sisältää se myös teknisiä ratkaisuja ja edellytyksiä laitoksen kyberturvallisuuden parantamiseksi. Suunnitelman perimmäinen tarkoitus on kuitenkin parantaa laitoksen teollisuus- ja automaatiojärjestelmin käytettävyyttä vähentämällä suunnittelemattomia käyttökatkoksia ja siten lisätä laitoksen tehokkuutta ja käyttöastetta.

Kuten opinnäytetyöstä voi havaita, kyberturvallisuuden haasteet liittyvät dokumentointiin, ihmisten toimintaan ja johtamiseen. Kyberturvallisuus ei ole tekninen ongelma, koska tekniik-

ka "taipuu" juuri sellaiseksi, kuin vaaditaan. Lisäksi toinen havainto on se, että mikään asia ei kehity itsestään ilman että sitä johdettaisi asianmukaisesti. Hyvään kyberturvallisuusasioiden johtamiseen kuuluvat laitoksen johdon sitoutuminen tavoitteisiin, asian organisointi ja resursointi, aikataulutus ja raportointi sekä pitkäjänteisyys (laitoksen pitkästä elinkaaresta johtuen).

Opinnäytetyössä esitelty menetelmä kyberturvallisuussuunnitelmasta ei tarvitse ottaa käyttöön koko kuvatussa laajuudessa yhdellä kertaa. Yksi etenemistapa voi olla, että suunnitelmasta käytetään aluksi ainoastaan niitä osia, joita tyypillisesti käytetään teollisuuden ohjaus- ja automaatiojärjestelmien elinkaaren alkupäässä (suunnittelu ja rakentaminen). Myöhemmin voitaisiin ottaa käyttöön ne suunnitelman osat, joita tarvitaan elinkaaren loppupäässä (käyttö ja operointi ja käytöstä poisto).

11 Oman osaamisen arviointi

Opinnäytetyön tekemisessä ongelmana ei ollut teollisuuden ohjaus- ja automaatiojärjestelmien kyberturvallisuuteen ja kehittämiseen liittyvät prosessit, johtamismallit tai tekniset menetelmät. Tämä johtuu siitä, että kirjoittajalla on asiasta kokemuspohjaista tietoa usean vuoden ajalta. Haasteena oli oikea käsittelytapa, joka vastaa sovittua tutkimusmenetelmää suhteessa esitettävään substanssiin. Eli opinnäytetyön kiinnostus haluttiin pitää itse substanssissa, eikä niinkään tutkimusmenetelmäosioissa. Toisaalta tämä oli uusi ja mielenkiintoinen tehtävä, joka pakotti kirjoittajan käsittelemään kyberturvallisuutta myös muusta kuin puhtaasti substanssinäkökulmasta.

Teollisuuden ohjaus- ja automaatiojärjestelmien kyberturvallisuudesta löytyy paljon julkisesti saatavilla olevaa informaatiota. Osassa on kaupalliset tarkoitusperät eli informaation avulla myydään joko suoraan tai välillisesti joitain alaan liittyviä tuotteita tai palveluita. Käytössä ei ole paljon sellaista informaatiota, joka perustuisi suoraan teollisuus ohjaus- ja automaatiojärjestelmien kyberturvallisuudesta vastuussa oleviin kokemuspohjaiseen tietoon. Kaupallisesti värittynyt informaatio keskittyy tyypillisesti ainoastaan yhteen osa-alueeseen, vaikka teollisuuden ohjaus- ja automaatiojärjestelmien kyberturvallisuus on monien eri osa-alueiden (johtaminen, jatkuva kehittäminen, prosessi, dokumentointi ja tekniset ratkaisut) summa.

Aiheeseen liittyvä teoriapohja on myös edelleen melko vähäistä. Toisaalta kyberturvallisuuden johtamiseen ja kehittämiseen pätevät samat lainalaisuudet ja viitekehykset kuin johtamiseen ja kehittämiseen yleisesti. Lisäksi laadunvalvonnan johtamisen ja kehittämisen alueella on paljon samankaltaisuuksia kyberturvallisuuden kanssa.

12 Jatkokehitysehdotukset

Teollisuuden ohjaus- ja automaatiojärjestelmiin liittyvän kyberturvallisuuden tilannekuvan kehittäminen voisi olla yksi luonnollinen jatkumo tälle opinnäytetyölle. Kattavan tilannekuvan luomiseen tarvitaan informaatiota historiasta eli tyypillisesti järjestelmälokeista, meneillään olevista tapahtumista eli informaatiota reaaliaikaisista sensoreista eri puolilta järjestelmäympäristöä sekä Internetin julkisista ja kaupallisista tietoturvaan liittyvistä tapahtuma- ja uhkasyötteistä (Feed). Lisäksi kaikelle em. informaatiolle tulee olla ympärivuorokautinen valmiustoiminto (SOC, Security Operation Centre), jossa on valmius aloittaa mahdolliset ennalta ehkäisevät tai korjaavat toimenpiteet.

Lisäksi em. toiminta tarvitsee teknisiä työkaluja, jotka on sovitettu teollisuuden ohjaus- ja automaatiojärjestelmille sopiviksi. Tällaisia ovat mm.:

- Automaattinen järjestelmäinventointi, joka kerää automaattisesti tarvittavat tiedot eri ohjaus- ja automaatiojärjestelmistä sekä hälyttää, mikäli järjestelmäympäristöön ilmestyy uusi laite/järjestelmä.
- Security Incident and Event Management (SIEM), eli tietojärjestelmä jonne keskitetään kaikki loki- ja reaaliaikainen tietoturvaan liittyvä tapahtumatieto eri järjestelmäsensoreilta sekä uhkasyöte Internetistä. Tämän järjestelmän avulla voidaan jopa ennakoida/ennustaa joidenkin tietoturvapoikkeamien tapahtuminen.

Lähteet

Kirjalliset lähteet

Suomen Automaatioseura Ry. 2013. Teollisuusautomaation tietoturva. Verkottumisen riskit ja niiden hallinta. Helsinki: Painomerkki Oy

Limnéll, J. & Majewski J. & Salminen, M. 2014. Kyberturvallisuus. Jyväskylä: Docendo.

Langner, R. 2011. Robust control system networks - How to achieve reliable control after Stuxnet. New York: Momentum Press.

Weiss, J. 2010. Protecting Industrial Control Systems from Electronic Threats. New York: Momentum Press.

VTT. 2010. TITAN-käsikirja. VTT:n päätuloksia Tekesin Turvallisuusohjelman TITAN-projektissa. Helsinki: Edita Prisma Oy.

Kananen, J. 2011. Kvantti: Kvantitatiivisen opinnäytetyön kirjoittamisen käytännön opas. Tampere: Tampereen Yliopistopaino Oy – Juvenes Print.

Sähköiset lähteet

Liikenne- ja viestintäministeriä (LVM). 2016. Verkko- ja tietoturvadirektiivi. Kansallista täytäntöönpanoa tukevan työryhmän loppuraportti. https://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/79770/LVM_09_2017_Verkko_%20ja_tietoturvadirektiivi.pdf?sequence=1

Turvallisuuskomitean sihteeristö. 2013. Suomen kyberturvallisuusstrategia ja sen taustamuistio. http://www.turvallisuuskomitea.fi/index.php/fi/component/dropfiles/?task=frontfile.download&id=5

Turvallisuuskomitean sihteeristö. 2013. Suomen kyberturvallisuusstrategian toimenpano-ohjelma. http://www.turvallisuuskomitea.fi/index.php/fi/component/dropfiles/?task=frontfile.download&id=21

European Union Agency for Network and Information Security (ENISA). 2011. Protecting Industrial Control systems. Recommendations for Europe and Member States. https://www.enisa.europa.eu/publications/protecting-industrial-control-systems.-recommendations-for-europe-and-member-states/at_download/fullReport

Swedish Civil Contingencies Agency (MSB). 2014. Guide to Increased Security in Industrial Information and Control systems. https://www.msb.se/RibData/Filer/pdf/27473.pdf

Centre for the Protection of National Infrastructure (CPNI). 2015. Manage Industrial Control systems Life Cycle. A Good Practice Guide. https://www.ncsc.gov.uk/content/files/protected_files/guidance_files/SICS%20-%20Manage%20ICS%20Lifecycle%20Final%20v1.0.pdf

Langner, R. 2013. To Kill a Centrufuge. https://www.langner.com/wp-content/uploads/2017/03/to-kill-a-centrifuge.pdf

Kuvat